Public Document Pack

Police Committee

Date: **THURSDAY, 2 NOVEMBER 2017**

Time: **11.00 am**

Venue: **COMMITTEE ROOMS, 2ND FLOOR, WEST WING, GUILDHALL**

Members:
Deputy Douglas Barrow (Chairman)
Deputy James Thomson (Deputy Chairman)
Nicholas Bensted-Smith
Deputy Keith Bottomley
Simon Duckworth
Emma Edhem
Alderman Alison Gowman
Christopher Hayward
Alderman Ian Luder
Andrew Lentin
Deputy Henry Pollard
Deputy Richard Regan
Lucy Sandford

Enquiries: **George Fraser**
tel. no.: 020 7332 1174
george.fraser@cityoflondon.gov.uk

Dates of next meetings:

- 15 December 2017
- 25 January 2018
- 1 March 2018
- 12 April 2018

Lunch will be served in Guildhall Club at 1PM
NB: Part of this meeting could be the subject of audio or video recording

John Barradell
Town Clerk and Chief Executive

AGENDA

Part 1 - Public Agenda

1. **APOLOGIES**

2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**

3. **MINUTES**
The draft public minutes from the last meeting.

For Decision

a) **Police Committee on 21 September 2017**

To agree

For Decision
(Pages 1 - 10)

b) **Professional Standards & Integrity Sub-Committee on 22 September 2017**

To receive

For Information
(Pages 11 - 14)

c) **Performance & Resource Management Sub-Committee on 26 September 2017**

To receive

For Information
(Pages 15 - 24)

d) **Police Pensions Board**

To receive

For Information
(Pages 25 - 28)

e) **Economic Crime Board on 20 October 2017**

To receive

For Information
(Pages 29 - 34)

4. **OUTSTANDING REFERENCES**
Report of the Town Clerk.

For Information
(Pages 35 - 40)

5. **HEALTH AND SAFETY ANNUAL PERFORMANCE UPDATE (1ST APRIL 2016-31ST MARCH 2017)**
Report of the Commissioner of Police

[*Appendix 3 of this report is included under item 23 of the agenda, as a non-public item*]

For Information
(Pages 41 - 62)

6. **CITY OF LONDON POLICE IT STRATEGY**
Report of the Chamberlain and Commissioner of Police

For Decision
(Pages 63 - 260)

7. **CAPITAL AND REVENUE BUDGET MONITORING REPORT TO SEPTEMBER 2017 - TO FOLLOW**
Report of the Commissioner of Police and the Chamberlain

[*This report was unavailable at the time of publication and will be circulated separately*]

For Information
(Pages 261 - 270)

8. **SPECIAL INTEREST AREA UPDATES**

For Information

a) **Public Order**

b) **Professional Standards & Integrity**

c) **Accommodation & Infrastructure**

9. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**

10. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**

11. **EXCLUSION OF THE PUBLIC**

MOTION - That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following items on the grounds that they involve the likely disclosure of exempt information as defined in Part I of Schedule 12A of the Local Government Act.

For Decision

Part 2 - Non-Public Agenda

12. **NON-PUBLIC MINUTES**

To agree the non-public minutes of the following meetings:

For Decision

a) **Police Committee on 21 September 2017**

To agree

For Decision
(Pages 271 - 276)

b) **Economic Crime Board on 20 October 2017**

To receive

For Information
(Pages 277 - 278)

13. **NON-PUBLIC OUTSTANDING REFERENCES**

Report of the Town Clerk

For Information
(Pages 279 - 280)

14. **ACTIONS TAKEN SINCE THE LAST MEETING**

Report of the Town Clerk

For Information
(Pages 281 - 284)

15. **POLICE ACCOMMODATION STRATEGY UPDATE**

Report of the City Surveyor, Chamberlain and Commissioner of Police

For Decision
(Pages 285 - 292)

16. **POLICE ACCOMMODATION STRATEGY: PHASE 3A BISHOPSGATE POLICE STATION REMAINING AREAS (TRANCHE 2) AND UPDATE ON TRANCHE 1 PROGRESS**

Report of the City Surveyor, Chamberlain and Commissioner

For Decision
(Pages 293 - 310)

17. **BRIDGE HOUSE ESTATES - FINSBURY HOUSE LETTING TO CITY OF LONDON POLICE - RECONCILIATION OF FUNDS**
Report of the Chamberlain

For Decision
(Pages 311 - 320)

18. **ID CRIME PROJECT**
Report of the Commissioner of Police

For Decision
(Pages 321 - 324)

19. **CCCI NICHE PROJECT-LEGACY DATA AND MOPI COMPLIANCE - ISSUE REPORT**
Report of the Commissioner of Police

For Decision
(Pages 325 - 338)

20. **HR UPGRADE TO V2015**
Report of the Commissioner of Police

For Decision
(Pages 339 - 342)

21. **COMPOSITE CLOSURE REPORT**
Report of the Commissioner of Police

For Decision
(Pages 343 - 368)

22. **ANNUAL WAIVERS REPORT 2016/17**
Report of the Chamberlain

For Information
(Pages 369 - 376)

23. **HEALTH AND SAFETY ANNUAL PERFORMANCE UPDATE (1ST APRIL 2016-31ST MARCH 2017) - APPENDIX 3**
This document is Appendix 3 of the report at Agenda item 5

For Information
(Pages 377 - 378)

24. **COMMISSIONER'S UPDATES**
Commissioner to be heard.

25. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**

26. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**

POLICE COMMITTEE

Thursday, 21 September 2017

Minutes of the meeting of the Police Committee held at the Guildhall EC2 at 10.30 am

Present

Members:

Deputy Douglas Barrow (Chairman)
Deputy James Thomson (Deputy Chairman)
Deputy Keith Bottomley
Emma Edhem
Alderman Alison Gowman
Christopher Hayward
Deputy Henry Pollard
Lucy Sandford

Officers:

David Clark	-	City of London Police
George Fraser	-	Town Clerk's Department
Alex Orme	-	Town Clerk's Department
Peter Kane	-	Chamberlain
Ian Dyson	-	Commissioner, City of London Police
Hayley Williams	-	Chief of Staff, City of London Police
Richard Jeffrey	-	Comptroller and City Solicitor's Department
Alistair Sutherland	-	Assistant Commissioner, City of London Police
Philip Gregory	-	Chamberlain's Department
Simon Rilot	-	City Surveyor's Department

1. **APOLOGIES**

Apologies were received from Simon Duckworth, Alderman Ian Luder and Nicholas Bensted-Smith.

2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**

a) **Minutes**

The Committee considered the minutes from the previous meeting, and Members agreed that there should be two amendments:

On Page 2, under item 4, Outstanding References, it should be clarified that the reference to the delay of the Annual Report referred specifically to its submission to the meeting of the Court of Common Council, which was postponed until September.

On Page 5, under item 8, Risk Register Update, it was agreed that the reference to the rollout date of the new CAD system as a risk if it remained

unknown should be removed. The Commissioner explained that it is not a risk and it is MPS dependent, and if it becomes a risk then will be managed as part of the ACs risk governance process.

On Page 5, under item 9, Special Interest Area Update, A Member asked when the new CoLP lead for Equality and Diversity would be appointed. The Assistant Commissioner stated that it had been advertised and if no one applied then he would post someone in there at the Force Strategic Workforce Planning meeting on 22 September. The Assistant Commissioner would update Members on any progress. (1)

RESOLVED – That the minutes be approved.

b) **Outstanding References**

The Committee considered a report of the Town Clerk that provided a summary of all the outstanding reference from the previous meetings of the Committee.

The Chairman stated his dissatisfaction with the prevalence of colour documents being printed in black and white. This comment was made in reference to the fact that some of the items within the table which were not yet marked as complete appeared to be greyed out when viewed in black and white within the agenda pack, thus reducing its clarity. The Chairman mentioned that this was an issue in later items within the agenda, such as items 5 & 8, in which graphs that had been designed to be viewed in colour were rendered ineffective. He requested that this issue be addressed, either by the production of packs in colour, or through the production of graphs with monochromatic printing in mind. (2)

A Member requested, in reference to OR 3, that the updates on the Police Accommodation Strategy that had been circulated to chairmen on behalf of the PAP Programme Director, be circulated to Members of the Police Committee. (3)

A Member requested, in reference to OR 8, that there needed to be an overview of all procurement to ensure that contracts are placed with ethical suppliers. The Chamberlain explained that there was a robust and substantial strategy in place, and agreed to send this to the Member. (4)

RESOLVED – That the report be received.

4. **STAFF SURVEY UPDATE**

The Committee received a report of the Commissioner of Police updating Members on the progress of the recent Staff Survey that had recently been completed.

The Commissioner explained to Members that this was the first survey that had taken place for a number of years, since 2014-15. He explained that, although it is still very early and the results have not been fully analysed yet, the initial findings have been positive.

The Assistant Commissioner explained that the survey had produced largely good news. He explained that the Survey had taken place in the summer of 2017 on the recommendation of the HMIC, and at the decision of the Chief Officer group.

The Assistant Commissioner explained that Chief Inspector Dave Evans would be putting forth an action plan from the findings, and that this would then be brought back to the Police Committee.

The Chairman illustrated his approval of the Force's swiftness in bringing this initial report to Committee, and his desire to see the final report at Committee. The Assistant Commissioner agreed that the final report would be submitted to the December meeting. (5)

A Member stated their approval at the conduction of the survey, and stated that the importance of a communication strategy amongst staff could not be underestimated.

The Chairman of the Professional Standards and Integrity Sub-Committee stated their approval of the completion of the survey, and stated that this should feed into the work of the Sub-Committee, playing an important role in informing the integrity plan with regards to important issues such as Code of Ethics and institutional culture.

RESOLVED – That the report be received.

5. **ANNUAL UPDATE ON THE CUSTODY OF VULNERABLE PERSONS (YOUNG PERSONS, CHILDREN AND MENTAL HEALTH)**

The Committee received a joint report of the Commissioner of Police and the Town Clerk that provided an update on the Custody of Vulnerable Persons.

The Chairman stated his dissatisfaction of the presentation of graphs which, when viewed in black and white in the hard copy of the agenda pack, were unclear. (2)

The Assistant Commissioner provided a verbal summary of the report content to Members, and explained that there was a substantial amount of detail in the report, with significant reference to mental health work, noting a rise in reported incidents involving mental health in the period from April 2016 to March 2017.

The Assistant Commissioner made a reference to paragraph 27, in which 4 young persons remained in Police custody when the local authority was unable to provide them with accommodation, and clarified that this was an example of a common issue taking place across all of London, not just within the City. The Chairman requested feedback on the status of the recovery of costs from the relevant local authority to the CoLP for overnight detention of these individuals. (6)

The Assistant Commissioner noted that there had been a rise in incidents involving the use of force. This was owing to the fact that handcuffs were applied at the scene rather than in the custody suite itself. He explained to Members that the decision to use handcuffs was as a result of a dynamic risk assessment at the time of the arrest / detention of the individual and dependent upon the officer's discretion. A Member noted that the figures were significantly higher as a percentage than those of other Forces used for comparison. The Assistant Commissioner explained that although CoLP showed a high percentage in the use of handcuffs, there had not been any rise in complaints made as a result of this, which would usually be seen as strong indicators of any problematic conduct issues. The Chairman of Professional Standards & Integrity Sub-Committee suggested that this might be an area relevant for the Sub-Committee.

A Member asked for further clarification of the figures for number of detainees as represented in Appendix 3, suggesting that they were in contradiction to those portrayed in the ADR. (7)

A Member requested confirmation that the City of London Corporation had signed *The Concordat for Children in Custody*. The Town Clerk agreed to follow this up. (8)

A Member requested information on the use of Tasers on under-18s, and how this was being recorded. The Assistant Commissioner explained that this was not covered by the report as the report was about detention, but would source an update for Members. He suggested that this also may be an area of focus for the Professional Standards & Integrity Sub-Committee. (9)

In reference to paragraph 44, A Member asked where the funding for the "street triage" system that was being piloted would be sourced from. The Commissioner agreed to follow this up and report back to Members. (10)

The Chairman noted that the graph in Appendix 1 was incomplete, with an arrow leading off the printed area, and asked if this could be rectified and re-circulated. (11)

In reference to paragraph 13, which describes the use of "the bubble" in the detainment of children and vulnerable people, the Deputy Chairman stated there was a need to look at improved custody options when the final refurbishments or upgrades under the accommodation programme take place. The Assistant Commissioner agreed that this was already a consideration but would ensure that the Deputy Chairman's comments were fed in to the Programme Director.

The Chairman noted the presence of "Not Known" results in the table within Appendix 4, corresponding to *Reason for a police vehicle being used* and *Method of transportation to first place of safety*. He explained that it was disappointing to see these but they were almost certainly as a result of the form not being filled in correctly and that the Force was trying to address this with first line supervision. In reference to Figure 10 of Appendix 2, a Member

explained that the high number assigned to the category "Other" was unhelpful. However, it was noted that this was a Home Office category not a Force category.

RESOLVED – That the report be received.

6. **QUARTERLY COMMUNITY ENGAGEMENT UPDATE**

The Committee received a report of the Commissioner of Police that updated Members on engagement activities across five main areas: Counter-Terrorism and communications, Safeguarding the Vulnerable, Prevention of Fraud, Anti-Social Behaviour, and Policing the Roads.

The Chairman stated that he was pleased with the work achieved as summarised within the report. He explained that there had been good Counter-Terrorism communications, referencing paragraph 1.14 of the report.

The Chairman requested that Members receive feedback of the results of the street triage scheme for which evaluation is due to be completed at the end of September, as referenced in paragraph 2.4 and 2.5 of the report. (12)

A Member asked for clarification on the "Levy" referenced in paragraph 4.4 of the report. The Chamberlain confirmed that this was in reference to the "Night-time Levy".

RESOLVED – That the report be received.

7. **STRATEGIC THREAT AND RISK ASSESSMENT (STRA) PROCESS 2017-18**

The Committee received a report of the Commissioner that provided Members with details of the Strategic Threat and Risk Assessment (STRA) process that had been undertaken by the City of London Police (CoLP) since 2016-17.

The Assistant Commissioner explained that this process has previously only been used for firearms and community policing, and that the CoLP is the first to use this process on a Force-wide basis. He explained that it was a positive step forward in operation, and that the Home Office has shown its approval.

In reference to paragraph 11 of the report, the Chairman requested confirmation of the date of completion of the Human Resources Workforce Plan. The Assistant Commissioner explained that this was due in October, following review.

RESOLVED – That the report be received.

8. **REVENUE BUDGET MONITORING REPORT TO JUNE 2017**

The Committee received a joint report of the Commissioner and the Chamberlain updating Members on the revenue budget to June 2017.

The Deputy Chairman queried one of the figures in Table 1, under the column for Q1 Actual, referring to the expenditure for ECD – Funded Units. (13)

The Commissioner explained that cash seizures referenced in paragraph 9 of the report led to additional costs to the Force as sums had to be repaid with interest. Although this was a regrettable result, lessons had been learned from this example case. The Chairman emphasised that it was important for the Force to accept that mistakes will sometimes be made, and that these should be seen as opportunities to learn.

The Commissioner explained that the Criminal Finance Act was a positive for the Force, enabling improvements to be made. He stated that as we have seen, following recent unforeseen events that have provided an additional challenge to the Force, making accurate predictions can be difficult.

The Chamberlain explained that the headline from the report was the end of year budget balance but that the numbers were volatile, which limited the confidence we could have in the forecast at this stage. The Chamberlain noted that paragraph 21 referenced a reserve of £3.4m that could then be utilised in the following year.

A Member noted that Risk Management appeared to have been well handled. The Chamberlain explained that the distinction between what were perceived to be costs and what were perceived to be risks had now been clarified.

A Member asked for further information about the funding for investment in innovation. The Commissioner explained that there was funding for 107 projects across policing as part of a large scale transformation. He explained that in the future it was likely that a significant portion of funding would be used to fund big tech investment.

RESOLVED – That the report be received.

9. **SPECIAL INTEREST AREA UPDATES**

a) **Strategic Policing Requirement Overview Update**

The Committee heard an update from the Strategic Policing Requirement Special Interest Area lead on recent developments.

The SIA Lead explained that CoLP was the first Force to employ the STRA process, before it became widely adopted. He stated that full credit must go to the senior management team, with particular mention of the T/Commander of Operations, Jane Gyford for her work in its execution.

The SIA lead emphasised the importance of not overlooking any actions and outcomes from the process which will lead to the evolution of Policing. He gave his approval of the process and gave thanks to the CoLP Head of Strategic Development, Stuart Phoenix for updates, illustrating that, since the last HMIC feedback recommended that there were areas requiring improvement, progress has been made.

RESOLVED – That the SIA Lead for the Strategic Policing Requirement Special Interest Area be heard.

b) **Counter-Terrorism Update**

RESOLVED – That the SIA Lead for Counter-Terrorism be heard.

10. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no questions.

11. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**
The Committee considered a report of the Town Clerk that requested their approval for the appointment of a new member, Mia Campbell, to the Professional Standards & Integrity Sub-Committee.

A Member noted that the reference to the expiration of the term of Lucy Sandford within the report should refer to Helen Marshall.

RESOLVED – That approval be given to the appointment of an external Member to the Professional Standards and Integrity Sub Committee, for a four year term commencing 22 September 2017, to reflect the decision of the selection panel made on 8 August 2017.

12. **EXCLUSION OF THE PUBLIC**
Members of the public were excluded.

13. **NON-PUBLIC MINUTES**
The Committee considered the non-public minutes from the last meeting on 13 July 2017.

RESOLVED – That the minutes be approved.

14. **REPORT OF ACTION TAKEN SINCE THE LAST MEETING**
The Committee received a report of the Town Clerk that updated Members on decisions taken under delegated authority or urgency powers since the last meeting on 13 July 2017.

RESOLVED – That the report be received.

15. **ACTION FRAUD INTERIM SERVICE PROVIDER WAIVER REPORT DOCUMENT REFERENCE NUMBER: WLOF0052**
The Committee received a report of the Commissioner of Police regarding the Action Fraud Service.

RESOLVED – That the report be received and the recommendations be approved

16. **ACTION FRAUD HOSTING INFRASTRUCTURE CONTRACT EXTENSION 22 AUGUST 2017 TO 22 JANUARY 2018 DOCUMENT REFERENCE NUMBER: WLOF0050**

The Committee received a report of the Commissioner of Police updating them on the approval of a waiver to extend the Virgin Media Action Fraud Infrastructure Hosting contract.

RESOLVED – That the report be received.

17. **DELOITTE DEMAND AND VALUE FOR MONEY REVIEW - OUTCOME UPDATE**

The Committee received a report of the Commissioner of Police providing Members with an update on the outcomes of the Deloitte Demand and Value for Money Review that looked at the balance of resources against current and future demand.

RESOLVED – That the report be received.

18. **DEMAND AND VALUE FOR MONEY REVIEW - SHORT TERM RECOMMENDATIONS AND NEXT STEPS**

The Committee received a report of the Commissioner of Police that sought Members' approval of action on short-term recommendations from the Deloitte Demand and Value for Money Review as outlined within the report.

RESOLVED – That the report be received and the recommendations be approved.

19. **ANNUAL UPDATE RAIL DELIVERY GROUP (RDG) CONCESSIONARY TRAVEL ARRANGEMENT**

The Committee received a report of the Commissioner of Police that updated Members on the Rail Delivery Group (RDG) Concessionary Travel Arrangement.

RESOLVED – That the report be received.

20. **RING OF STEEL AND SECURE CITY PROGRAMME (FORMERLY ONE SAFE CITY) UPDATE**

The Committee received a report of the Commissioner of Police that updated them on the Ring of Steel and Secure City Programme (Formerly One Safe City) Update.

RESOLVED – That the report be received.

21. **POLICE ACCOMMODATION VERBAL UPDATE**

The Committee heard a verbal update from the City Surveyor on the progress of the Police Accommodation Strategy.

RESOLVED – That the City Surveyor be heard.

22. **COMMISSIONER'S UPDATES**

The Committee heard a verbal update from the Commissioner of Police on the recent activity since the last meeting.

RESOLVED – That the Commissioner be heard.

23. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no questions.

24. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**
There were no further non-public business.

The meeting closed at 12.40 pm

Chairman

Contact Officer: George Fraser
tel. no.: 020 7332 1174
george.fraser@cityoflondon.gov.uk

This page is intentionally left blank

PROFESSIONAL STANDARDS AND INTEGRITY SUB (POLICE) COMMITTEE

Friday, 22 September 2017

Minutes of the meeting of the Professional Standards and Integrity Sub (Police) Committee held at the Guildhall EC2 at 1.45 pm

Present

Members:

Alderman Alison Gowman (Chairman)
Tijs Broeke
Lucy Sandford (External Member)
Deputy James Thomson (Ex-Officio Member)

Officers:

George Fraser	-	Town Clerk's Department
Alex Orme	-	Town Clerk's Department
Richard Jeffrey	-	City Solicitor
Nirupa Gardner	-	Internal Audit
Stuart Phoenix	-	Head of Strategic Development, CoLP
Dermont Robinson	-	Director of Professional Standards, CoLP
Alistair Sutherland	-	Assistant Commissioner, CoLP

1. **APOLOGIES**
   Apologies were received from Deputy Doug Barrow, Nicholas Bensted-Smith and James Tumbridge.

2. **DECLARATIONS BY MEMBERS OF PERSONAL OR PREJUDICIAL INTERESTS IN RESPECT OF ITEMS TO BE CONSIDERED AT THIS MEETING**
   There were no declarations.

3. **MINUTES**
   Members considered the public minutes from the last meeting, held on 5 June 2017.

   RESOLVED – That the minutes be approved.

MATTERS ARISING

The Chairman welcomed new Member, Tijs Broeke, to his first meeting of the Sub-Committee.

The Chairman noted that the agenda packs had been printed in their entirety on blue paper, thus signifying confidential status. The Town Clerk explained that due to printing protocol prohibiting confidential papers from being bound with non-public or public papers, it had previously been advised to print packs purely on blue paper for the purpose of the meeting. The Chairman requested that

packs be printed separately in correct accordance with their visibility classification to ensure that the tradition of the City Corporation is maintained. The Town Clerk confirmed that all future agendas for the Sub-Committee would be printed and bound in separate packs as per her request. (1)

4. **INTEGRITY DASHBOARD AND CODE OF ETHICS UPDATE**

The Sub-Committee received a report of the Commissioner of Police providing Members with an update on the Integrity Dashboard and Code of Ethics issues.

The Head of Strategic Development explained that a full report illustrating the results from the recent Staff Survey will be published in the coming weeks. He explained that an initial report had been submitted to the Police Committee on 21 September. The Chairman requested that this be circulated to all Members of the Sub-Committee that do not sit on the Police Committee. (2)

The Head of Strategic Development explained that the Integrity Standards Board had considered the addition of 5 new dashboard indicators around sponsorship as a result of the new Standard Operating Procedures (SOP).

A Member asked if there were minutes available from the London Police Challenge Forum. The Head of Strategic Development confirmed that there were, and that these could be submitted to the next meeting agenda. (3)

In reference to paragraph 11 of the report, a Member asked for further explanation on how the Force was dealing with whistleblowing. The Assistant Commissioner explained that a “bad apple” system was in place, allowing for confidential reporting through an online portal. He also clarified that a lack of online reports logged did not necessarily mean that reports weren’t being received via other means. The Chairman explained that the new ability to respond to anonymous reports with follow-up questions was very beneficial. The Director of Professional Standards explained that there were two systems in place, with the “bad apple” system active for 2-3 months at this point. He explained that there was a whistleblowing policy in place, and that there were now an increased number of non-anonymous reports being submitted to the Professional Standards Directorate. He explained that they were managing to raise awareness with other Forces, and that this was a positive step. He offered to report back to the Sub-Committee on this as required. The Deputy Chairman stated that it was useful to know that these were coming through.

The Head of Strategic Development explained that the next meeting of the London Police Challenge forum would take place on 5 December 2017, from 10:00-13:00. He agreed to circulate a note to remind members of this prior to the event. (4)

RESOLVED – That the report be received.

a) **Integrity Dashboard - 2017/18 Q1**

The Sub-Committee received a report of the Commissioner of Police providing the latest figures surrounding the Force Integrity Indicators.

RESOLVED – That the report be received.

b) **Police Integrity Development and Delivery Plan Report 2016-17**

The Sub-Committee received a report of the Commissioner of Police updating Members on the Police Integrity Development and Delivery Plan.

The Head of Strategic Development explained that a report of Crime Audits being looked into would be submitted to the following meeting. (5) The Chairman asked for clarification that this was independent of the Staff Survey report, and this was confirmed to be the case.

A Member asked for an explanation of the column headings "V1, V2 etc."" within the report. The Head of Strategic Development explained that these were analogous to "Q1, Q2 etc.", and referred to the word "version" rather than "quarter". A Member asked for confirmation that this was aligned to the quarters of the financial year of the UK, commencing on 1 April, and this was confirmed to be the case.

Measure 1.9 – To ensure training on standards, values and leadership roles is available for all staff

The Chairman asked how the training was being monitored. The Head of Strategic Development confirmed that the courses were checked off as complete during the induction process.

Measure 1.10 – To adopt Authorised Professional Practice (APP) and national guidance for Force policies and procedures

The Chairman asked if there was a deadline for completion of the review of all policies and procedures. The Head of Strategic Development explained that the report of policies that require updating would be considered next week at the meeting of the Performance & Resource Management Sub-Committee.

The Chairman noted that there was an error on the CoLP website that stated that referred to "Corporate pay 2015/16", when it should refer to "2016/17", and asked that it be corrected. (6)

A Member asked if the level of transparency provided by the CoLP regarding the publishing of Gifts & Hospitality was superceded by any other forces. They suggested that the Gifts & Hospitality report be published and made clearly visible on the CoLP website. Those present agreed that this would be beneficial. (7)

5. **QUESTIONS RELATING TO THE WORK OF THE SUB-COMMITTEE**

There were no public questions.

6. **ANY OTHER BUSINESS THE CHAIRMAN CONSIDERS URGENT**

There was no further public business.

7. **EXCLUSION OF THE PUBLIC**

RESOLVED - That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following items on the grounds

that they involve the likely disclosure of exempt information as defined in Part I of the Schedule 12A of the Local Government Act.

The meeting closed at 3.36 pm

Chairman

Contact Officer: George Fraser
tel. no.: 020 7332 1174
george.fraser@cityoflondon.gov.uk

PERFORMANCE AND RESOURCE MANAGEMENT SUB (POLICE) COMMITTEE

Tuesday, 26 September 2017

Minutes of the meeting of the Performance and Resource Management Sub (Police) Committee held at the Guildhall EC2 at 1.45 pm

Present

Members:

Deputy James Thomson (Chairman)	Kenneth Ludlam
Nicholas Bensted-Smith	Caroline Mawhood
Tijs Broeke	Lucy Sandford (External Member)

Officers:

Paul Adams	-	CoLP
Neil Davies	-	Town Clerk's Department
George Fraser	-	Town Clerk's Department
John Galvin	-	Town Clerk's Department
Alex Orme	-	Town Clerk's Department
Jeremy Mullins	-	Chamberlain
Stuart Phoenix	-	Head of Strategic Development, CoLP
Andrew Ricketts	-	CoLP
Alistair Sutherland	-	Assistant Commissioner, CoLP
Hayley Williams	-	CoLP

1. **APOLOGIES**
   Apologies were received from Deputy Doug Barrow, Deputy Keith Bottomley and Alderman Alison Gowman.

2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**
   There were no declarations.

3. **MINUTES**
   The Sub-Committee considered the minutes from last meeting, held on 30 May 2017.

   Item 5 – Outstanding References
   The lead member for anti-social behaviour (ASB) explained that she was still in the process of looking into the improved presentation of ASB data to aid Members' understanding. (1)

   Item 7 – HMIC Update Report
   The Chairman requested that a standing item for information be added to future agendas providing an update to Members on the progress relating to the Deloitte review. (2) The Assistant Commissioner explained that reassurance

was given by the STRA report that 12 “quick wins” could be achieved with no extra resource requirements.

Item 10 – Internal Audit Update Report
It was agreed that a Project Management audit report, as mentioned at the last meeting, should be submitted to the next meeting of the Sub-Committee. (3)

RESOVLED – That the minutes be approved.

4. **OUTSTANDING REFERENCES**
The Sub-Committee received a report of the Town Clerk that summarised the outstanding actions from previous meetings.

OR3 – Guidelines to ASB Data
It was agreed that this item was still outstanding

OR6 – Licensee Responsibility for CCTV
The Chairman explained that the comments about the Licensing Committee not being supportive were surprising. The Assistant Commissioner stated that he was also surprised by this, and agreed to follow it up.

OR8 – Forecasting Status Changes
The Chairman requested that this item remain “Ongoing”.

RESOLVED – That the report be received.

a) **Briefing Note - OR 9 - CoLP Policy Oversight Annual Update 2016-2017**

OR9 – Newly RED Status Indicator
The Chairman requested that dates be added for closedown of items within the table. The assistant Commissioner explained that there would be specific dates for Health & Safety and Force Vetting, and agreed to include confirmed closedown dates by the next meeting.

b) **Briefing Note - OR 10, OR 12 - Performance Against Measures**

A Member welcomed this report, but stated his disappointment that it had taken so long to arrive. He noted that they seemed to be carrying out less surveys. The Assistant Commissioner explained that they had experienced survey fatigue, and were considering commissioning an external party to carry out surveys. He explained that Corporate Communications would deliver the next survey in November 2017. A Member stated that the issue was not whether or not an internal or external provider would deliver the survey, but rather to identify the correct area to survey. The Assistant Commissioner explained that this was the aim, and identifying the correct area to survey would be the task of Corporate Communications.

A Member explained that the method of survey carried out was crucial, and getting business Members to respond can be very hard. The Assistant

Commissioner agreed and explained that perhaps a narrower target audience would be more effective. The Member explained that having targeted questions would make respondents more likely to engage. The Chairman requested clarification on the dates of surveys. The Assistant Commissioner explained that this could be confirmed at the next meeting. (4)

5. **INTERNAL AUDIT UPDATE REPORT**

The Sub-Committee received a report of the Chamberlain providing Members with an update on the work of the Internal Audit that has been undertaken by the CoLP since the last report in May 2017.

The Chairman noted that there seemed to be slippage, and that a number of reports appeared to be 6 months out of date. The Chairman asked for an update on this. The Chamberlain explained that these outstanding reports are at the stage in which they have yielded some conclusions, but are awaiting discussion with the Commissioner before they can be finalised.

The Chairman asked if those marked as RED would have responses confirmed and the recommendations followed up. A Member stated that RED/AMBER statuses do not provide a tangible feel for the true status, and suggested that increased background information and context would be useful. The Chamberlain explained that all those marked as completed, had indeed been provided with background information at previous meetings.

In reference to paragraph 9, a Member asked for an update on why no security patches had been installed since 2015. The Chamberlain explained that they were working with the IT department on wide ranging issues with the transformation programme, within which this was included. He explained that old patches do not apply to new technological systems. He explained that Audit & Risk had just released a report on IT transformation developments. The Chamberlain suggested that this be circulated to Members. (5) The Chairman showed his concern over the length of time the It project had been deferred for.

The Chairman asked that all the outstanding reports be completed. (6) The Chamberlain explained that many of the reports were essentially complete, though were awaiting completion of testing with Town Clerk's department. He explained that there was a fear of providing inaccurate recommendations if this was not done.

A Member suggested that it might be useful to provide a comment on why/who decided that the reports should be deferred. The Chamberlain explained that in the case of Action Fraud, they were awaiting the Interim Service. The Chairman requested confirmation that discussion would take place at the end of December 2017, when the interim service ends. The Chamberlain confirmed that this was the case.

The Chamberlain explained that the definition of Project v Programme was crucial due to the definition of costs. He explained that a Programme was very hard to allocate budgets at high levels. The Chairman requested that the

Chamberlain enter discussion with the Commissioner before updating the report. He emphasised that it would be very beneficial to the broader agenda. The Chamberlain confirmed that this would be available at the next meeting. (7)

The Chairman noted an error within the table of the report where the total red column was populated by “Green” and “Amber”, rather than digits. The Chamberlain confirmed that in both cases, the table should read “0”.

RESOLVED – That the report be received.

6. **HMICFRS INSPECTION UPDATE**

The Sub-Committee received a report of the Commissioner of Police that provided Members with an update on the HMICFRS Inspection.

The Assistant Commissioner explained that good progress had been made, with 16+ new areas marked as GREEN, and 10 left as RED.

The Assistant Commissioner explained that the HMIC had extended its remit to include inspections of fire and rescue services in England, leading to its new title of HMICFRS. He explained that no reports in the last period had been published on the CoLP.

The Assistant commissioner explained that an inspection on “effectiveness” was upcoming and would last for 3 days.

The Assistant Commissioner explained that many of the indicators were essentially ready to move to GREEN status. The Chairman requested that closedown timelines are included for all open indicators. (8)

The Chairman asked for information on the approach taken by HMICFRS towards inspections. The Head of Strategic Development explained that they were moving towards basing them on “Force Management Statements”, with the launch of requirements taking place on Monday 2 October. The HMICFRS would look at crime data before making a decision on which areas to inspect. He explained that the CoLP were in a strong position due to the STRA process. He explained that there would continue to be thematic inspections alongside one-off inspections.

A Member asked about the status of Stop and Search data. The Assistant Commissioner credited the team for their improvements to management of systems for Stop & Search data.

A Member asked about the status of the Deloitte review of workforce, which was marked as RED under an area for improvement within the report. The Assistant commissioner explained that this was imminently about to move into GREEN status. He explained that Officer Skills and Training Database systems were due to go live in October 2017.

The Chairman asked for confirmation of what was meant by “internal deadline”. The Assistant Commissioner explained that this was used in cases where

HMICFRS did not provide their own deadline. The Chairman asked for confirmation that this meant there had not been deadlines missed or postponed, and the Assistant Commissioner confirmed this, citing the use of RED status.

The Chairman asked if specific dates would be more appropriate than marking as “immediate”. A Member asked if this meant that the work had not been done. The Head of Strategic Development explained that these were used in cases in which disclosure issues exist, leading to reviews in these areas (regardless of the issues not being those of CoLP).

The Chairman asked for confirmation that Stop and Search indicators would move from RED to GREEN with the introduction of “Niche” in November 2017. The Assistant Commissioner confirmed that this was the case.

The Chairman asked for confirmation of when the Police Legitimacy indicators currently marked as RED would move to GREEN. The Assistant Commissioner explained that both of these are expected to move to GREEN in December 2017.

The Chairman asked for timeframes on the tri-service review of the joint emergency services interoperability principles indicators moving to GREEN. The Assistant Commissioner explained that multiagency programmes such as these pose significant challenges with regards to connecting timelines, and as a result it would be very difficult to predict future dates of completion. The Chairman noted that therefore not all statuses were ready to go GREEN. The Assistant Commissioner explained that this was the case only due to reliance on other forces to coordinate. The Head of Strategic development explained that the CoLP’s regime is limited by the calendar of integration with 3 other forces and how they are able to feed back.

A Member illustrated their concern at the comments made regarding Organised Crime under the Police Effectiveness section. The Assistant Commissioner explained that a significant amount of work had been done alongside the Metropolitan Police Service to map this out. He explained that improvements had been made over the last 6-9 months, and that a large proportion of the issues were related to decisions around funding. He explained that these issues were prevalent nationally. The Commissioner explained that this was a new area of focus for CoLP, and that it was linked to the London model. He confirmed that there had not been any indication to alert CoLP of dangers based on the 2016 reviews. The Chairman asked that REDs included more detailed comments for Members in future.

RESOLVED – That the report be received.

7. **1ST QUARTER PERFORMANCE AGAINST MEASURES SET OUT IN THE POLICING PLAN 2017-20**

The Sub-Committee received a report of the Commissioner of Police that summarised performance against measures in the Policing Plan 2017-20 for the period 1 April 2017 to 30 June 2017.

The Assistant Commissioner explained that there had been a regrettable rise in victim-based crime, in correlation with national figures. He explained that there was a focus particularly on vulnerability.

The Assistant Commissioner asked Members to note the allocation of resources to terror attacks in Manchester and London.

A Member asked why there had been increases in 3 crime areas, and the Assistant Commissioner explained that a threat matrix was responsible for allocation of resources. With the current threat level unlikely to go down soon, there is a need to adapt.

A Member asked if more people would be encouraged to commit crimes based on increased success. The Assistant Commissioner explained that repeat offenders sometimes persist for as long as 20 years in some of these crime areas, and that a small number of offenders were responsible for a large volume of crimes. The Assistant Commissioner explained that there are an increased number of CID officers on the street in uniforms, with the idea that prevention can replace investigation in many cases.

A Member asked if the focus had changed since the last Operation Mass event. The Assistant Commissioner agreed to follow this up to confirm. (9)

The Chairman asked for data surrounding “capability” and “impact” to be sourced, as both were highlighted within the report summary. (10)

The Assistant Commissioner explained that Moped crime was popular as it was both lucrative and provided means for easy escape from the scene. He also explained that, similar to acid attacks, the crime was part of a trend. He explained that the offenders were generally not residents of the City of London, so the challenge was in keeping them out.

The Assistant Commissioner suggested that perhaps it would be beneficial to invest in the reporting of Counter-Terrorism, rather than in uniformed policing.

The Chairman noted that the table illustrating Cyber Crime NFIB referrals was incomplete. A Member asked for confirmation of what NFIB referrals were, and requested that they review which/how data is presented to the Sub-committee, as in many cases it was unclear. (11)

A Member noted that “None of the above” was the most common code, referring to 15 reports. Members agreed that this was not useful.

A Member asked for clarification on whether 75% was a positive figure for satisfaction of ECD service. The Assistant commissioner explained that the majority of fraud offences don’t result in a challenge, and rather they contributed data to the bigger picture. He explained that they focused more on victim-care with additional investment now. There has been a lot of work

outsourced to multiple external agencies, and therefore quality control is difficult.

The Assistant Commissioner suggested that the T/Commander of Economic Crime attend the following meeting in order to explain further. (12)

A Member asked for clarification on what a “binary option” was. The Chairman stated that details such as these should be provided within reports to aid Members, as mentioned previously.

The Assistant Commissioner explained that the nature of Vulnerability meant that there was less resources on the street, and thus was a growing issue. A Member asked where these resources were being allocated. The Assistant Commissioner explained that there was a wide catchment, including begging, mental health issues and domestic problems.

In reference to the graph illustrating the Number of Victim-Based Violent Crimes per Month, the Chairman asked for confirmation that there were seasonal patterns. The Assistant Commissioner confirmed that this was the case.

A Member asked about the traffic management of Bank junction in relation to cyclists, considering recent incident in which a cyclist killed a pedestrian. The Assistant Commissioner explained that there was not as much policing of cyclists as desired, however, the CoLP was working in cooperation with the Road Danger Reduction Plan. A Member noted the large volume of cyclists, citing this as a cause for consideration. The Assistant Commissioner explained that it had been challenging to maintain management in line with the significant influx of cyclists since the London 2012 Olympics. He explained that only those cyclists whose actions warrant criminal investigations can be addressed by the CoLP. A Member noted that the perception of cyclists as irresponsible was increasing, and efforts needed to be made to raise awareness of the efforts that have been undertaken to address the issue.

The Chairman asked what was meant by a “Layering Approach”. The Assistant Commissioner explained that this meant using various operations/crimes to build a wider view of a suspect or offender.

In reference to Public Order and Protective Security, the Assistant Commissioner explained that HR was due to look at public order training. He explained that there was a consideration of an incentivisation payment as a result of reduced interest in the training.

A Member asked if the CoLP charge for specific events such as Marathons taking place within the City boundaries. The Assistant Commissioner explained that there was some cost recovery, but this was a contentious issue. The Chairman asked if protests were included in these statistics, and upon the Assistant Commissioner’s confirmation that they were not, requested these be produced for the next meeting. (13)

A Member explained that they had been made aware that arrests had dropped by 55% nationally since 2008, and asked for confirmation that this was correct. The Assistant Commissioner stated that he could not confirm that this statistic was correct, but explained that the grounds for arrest had been tightened, with notices being increasingly supplied in their place on the street.

RESOLVED – That the report be received.

8. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no questions.

9. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**
There was no further business.

10. **EXCLUSION OF THE PUBLIC**
RESOLVED – That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following items on the grounds that they involve the likely disclosure of exempt information as defined in Part 1 of the Schedule 12A of the Local Government Act.

11. **NON-PUBLIC MINUTES**
The Sub-Committee considered the non-public minutes from the last meeting, held on 30 May 2017.

Members requested that the One Safe City update report due to be submitted to the next meeting of the Police Committee, be submitted to the next meeting of the Performance and Resource Management Sub-Committee, on 30 November 2017. (14)

RESOLVED – That the non-public minutes be approved.

12. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no non-public questions.

13. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE SUB-COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**
There was no further non-public business.

The meeting closed at 3.25 pm

Chairman

Contact Officer: George Fraser
tel. no.: 020 7332 1174
george.fraser@cityoflondon.gov.uk

This page is intentionally left blank

POLICE PENSIONS BOARD

Monday, 2 October 2017

Minutes of the meeting of the Police Pensions Board held at the Guildhall EC2 at 11.00 am

Present

Members:

Alderman Ian Luder (Chairman)	John Todd (Deputy Chairman)
Helen Isaac	Alexander Barr

Officers:

Caroline Al-Beyerty	-	Chamberlain's Department
George Fraser	-	Town Clerk's Department
Jeff Henegan	-	Chamberlain's Department
Graham Newman	-	Chamberlain

1. **APOLOGIES FOR ABSENCE**
   Apologies were received from Kieron Sharp and Davina Plummer.

2. **MEMBERS DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**
   There were no declarations.

a) **Minutes**

The Board considered the minutes from the last meeting held on 10 May 2017.

The Chairman noted that under Item 4 of the minutes, City of London Police Pension Scheme Update, it referred to a comment that stated the number of deferred scheme members as approximately 700. It was discussed and confirmed that the correct number, as referred to within Item 5, Appendix 5 on the current agenda, was 253.

The Chairman queried whether it would be appropriate to send a letter to request updated contact details from all those that have left prior to receiving letters detailing their entitlements – this would enable the scheme to record the number of those that are deemed to be “out of contact”. The Pensions Administrator explained that this would likely require contacting all deferred scheme members.

The Deputy Chairman illustrated his concern with adhering to regulation in the face of an audit process if there is a lack of attempted communication to deferred members. The Deputy Chairman also queried whether subsequent marriage was an issue affecting eligibility of deferred members. The Pensions administrator explained that marriage would not affect the eligibility of members

to the scheme, and emphasised that attempting to keep in touch should always be a priority. The Deputy Chairman stated his approval that significant efforts were being made in this regard.

MATTERS ARISING

The Deputy Chairman asked for confirmation that his appointment as Deputy Chairman had been reported to the Police Committee Members and the Chairman confirmed that this was the case.

RESOLVED – That the minutes be approved.

b) **Outstanding References**

OR1 – Annual Report to Grand Committee
The Chairman explained that the annual report to Police Committee should be submitted to the January meeting, and marked as due by the next meeting of the Board on 9 January.

The Deputy Chairman noted that the date of the previous meeting cited within the Outstanding References document was 30/05/17, where it should read 10/05/17.

OR2 – Issuing of Pensions Savings Statements
The Chairman explained that the Annual Benefits statements action should be split between two elements here – the Issue of Annual Statements by the end of August which should now be complete, and the Issue of Pension Saving Statements by the end of October. The Pensions Administrator confirmed they were unable to comply with the requirement to issue a Pension Statement by the date specified in the schedule, due to both software issues and the absence of a pension manager. A Member expressed concern that missed deadlines had not been explicitly identified by the covering report, and asked for clarification as to whether or not this apparent breach required reporting to The Pensions Regulator. (1)

RESOLVED – That the report be noted.

4. **WORK PROGRAMME**
The Board considered a report of the Town Clerk that summarised the proposed work programme of the Police Pensions Board.

RESOLVED – That the report be noted.

5. **POLICE PENSIONS SCHEME UPDATE**
The Board considered a report of the Chamberlain that provided Members with an update on activity of the Police Pension Scheme since the last meeting.

The Chairman queried the first sentence of the second paragraph of the letters in Appendices 2a and 2b, suggesting that it read: “Your deferred pension has been based on length of service and qualifying pensionable pay over the last

12 months of service". A Member suggested that a footnote was included for clarity. The Chamberlain suggested that perhaps the inclusion of an example would be helpful.

A Member queried the mention of the "cost-of-living index" within the letters, and requested confirmation that this was the relevant index to use. A Member explained that this should reflect the wording of the PMB and agreed to confirm this. (2)

The Chairman explained that he was pleased with the additional paragraph relating to the offering of advice as illustrated within Appendix 3.

The Deputy Chairman asked for clarification of who makes the decision within the Internal Dispute Resolution Procedure (IDRP). The Pensions Administrator explained that the Corporate Treasurer made this decision, and if it cannot be resolved at this point then it would go to the financial ombudsman.

The Chairman explained that Appendix 4, Risk Register, was too small to read clearly.

The Chairman queried the risk of Pension Fraud moving from Serious to Minor, and the Chamberlain explained that this was the target risk, rather than current risk.

A Member asked whether the heavy reliance on external trainers should be viewed as a risk. The Chairman explained that they are reliant on having the appropriate level of training. The Chamberlain explained that there is a Member group that carries out checks on Barnet Waddington to fulfil mitigation, as well as Financial Investment Board oversight. The Chairman concluded that although they are reliant on external training, the mitigation measure if to ensure that the trainers are competent.

The Deputy Chairman explained that there was a new campaign released by The Pensions Regulator (TPR) to improve standards of governance by making communication more clear and directive. He explained that this should be circulated to Board Members. (3)

The Chairman queried whether Data Protection Training would be necessary for Board Members. He asked whether or not this training was run centrally for Corporation Staff, and if it would be considered a risk if Members didn't make themselves available for training. (4)

In reference to Appendix 5, the Deputy Chairman asked for clarification over "eligible children". The Pensions Administrator explained that the child would be eligible until the age of 23, and that child's parent died, then they may perhaps be eligible for life.

The Deputy Chairman asked whether The Pensions Regulator was due to receive the minutes of the Police Pensions Board. It was confirmed by the Chairman that the minutes would be provided if necessary under challenge.

RESOLVED – That the report be received.

6. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE BOARD**
There were no questions.

7. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**
There was no further business.

8. **EXCLUSION OF THE PUBLIC**
Members of the public were excluded.

9. **TRAINING UPDATE**
The Board received an update on training provision to Members that summarised the analysis carried out since the last meeting.

RESOLVED – That the report be received.

10. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB-COMMITTEE**
The Chairman requested that the date of the next meeting be added as an item to the agenda in future. (7)

There were no other non-public questions.

11. **ANY OTHER NON-PUBLIC BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**
There was no further non-public business.

The meeting closed at 11.47 am

Chairman

Contact Officer: George Fraser
Tel.No.: 020 7332 1174
george.fraser@cityoflondon.gov.uk

ECONOMIC CRIME BOARD OF THE POLICE COMMITTEE

Friday, 20 October 2017

Minutes of the meeting of the Economic Crime Board of the Police Committee held at the Guildhall EC2 at 11.00 am

Present

Members:
Deputy Tom Sleigh (Acting Chairman)
Deputy Keith Bottomley
Deputy Robert Merrett

Officers:

George Fraser	-	Town Clerk's Department
Oliver Bolton	-	Town Clerk's Department
Glenn Maleary	-	Detective Chief Superintendent, CoLP
Pauline Smith	-	Head of Action Fraud, CoLP

1. **APOLOGIES**
Apologies were received from Deputy Doug Barrow, Deputy James Thomson, Simon Duckworth, Nicholas Bensted-Smith and Deputy Henry Pollard.

2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**
There were no declarations.

3. **MINUTES**
Members considered the Public Minutes from the last meeting, held on 27 July 2017.

RESOLVED – That the minutes be approved.

4. **OUTSTANDING REFERENCES**
Members received a report of the Town Clerk summarising the outstanding actions from previous meetings.

OR3 – Cyber Training for Members
In light of the example training session provided within the agenda, a Member queried the feasibility of providing training to Members. The Detective Chief Superintendent suggested that it might be beneficial to invite a representative of the Economic Crime Academy to the following meeting in order to present and discuss feasible cyber training provision for Members. (1)

It was also requested that an update be provided to Members on the current provision of cyber training to City Corporation staff. (2)

RESOLVED – That the report be received.

5. **ECONOMIC CRIME VICTIM CARE UNIT (ECVCU) PRESENTATION**

Members received verbal and written report updates on the Economic Crime Victim Care Unit (ECVCU) from the Commissioner of Police.

The Head of Action Fraud explained that the ECVCU was an initiative run in partnership between the CoLP, MPS and Action Fraud, with the BTPA recently dropping out as a result of having no victims. The service had been funded for the last three years by the Mayor's Office for Police and Crime (MoPAC).

The Head of Action Fraud explained that the focus was on the 5% most vulnerable victims, and that a survey had been carried out recently to gauge desire for the service. The Head of Action Fraud explained that a 92-year old man had travelled from Surbiton to illustrate his approval of the service. She explained that they had confirmed 18 cases in which the "re-scamming" of victims had been averted when followed up over a year later.

The Head of Action Fraud explained that the Mayor's Office for Police and Crime (MOPAC) had provided funding to enable a trial of a national roll-out involving Greater Manchester Police and the West Midlands Police. She explained that there was a desire to ensure the success of the service prior to rolling out under the umbrella of Action Fraud. An evaluation of the service by Age UK will yield findings in April 2018.

A Member asked how this service would link to the Action Fraud Victim Service. The Head of Action Fraud explained that this service was a provision for all those victims that had not received any service. She explained that the Victim Service demands the "soft skills" that victims require in order to feel supported from an emotional perspective, whilst the ECVCU provides the more technical Economic Crime skills and knowledge that needs to be complimented by this. The desire would be to combine the two services, with the support of MOPAC, in order to provide seamless support for victims of economic crime.

The Chairman asked what factors determined that someone would be declared "vulnerable". The Head of Action Fraud explained that they would view that person's current situation in relation to the crime. This includes judging how much the sum of money lost would negatively affect their life. A Member declared that the business case for funding should be centred on victims' vulnerability.

The Chairman asked what the total funding available was for Action Fraud. The Head of Action Fraud explained that it was around £1m, with a possible increase to £1.7 the following year. A Member noted that this was a significant sum, and asked how many staff this covered. The Detective Chief Superintendent of Economic Crime explained that this made provision for 23 staff Members as well as service costs.

The Chairman asked what could be done by Members to support Action Fraud. The Head of Action Fraud explained that any value added to Policing on a wider basis would help Action Fraud. The Detective Chief Superintendent of

Economic Crime explained that the victim code of conduct dictates that a minimum level of service is provided to victims, and that in order to maintain this standard support of victim care initiatives was crucial. The Town Clerk explained that there has been movement to engage with PCCs and APCC to increase collaboration, towards which there has been Member input. The Chairman stated his approval of this as a good example of pan-London working, and recommended that Members are supportive.

RESOLVED – That the Head of Action Fraud be heard.

6. **NATIONAL LEAD FORCE: 2017/18 PERFORMANCE REPORT**

The Board received a report of the Commissioner of Police outlining the quantitative and qualitative performance of the City of London Police as the National Lead Force for Fraud between April 2017 and September 2017.

The Detective Chief Superintendent of Economic Crime explained that a 7% Year-to-date (YTD) increase in the number of crimes reported to Action Fraud amounted to 9,000 victims. He explained that all economic crime was under-reported, and so there is an assumption that increased awareness is the basis behind a consistent increase in reported crimes.

The Detective Chief Superintendent of Economic Crime explained that staff retention was an inherent challenge due to the nature of the work and the value of the skills required to tackle Economic Crime.

The Detective Chief Superintendent of Economic Crime explained that an effort to improve the clarity and simplicity of reporting lines was expected to increase lines of enquiry. There has also been a concerted effort to engage nationally, where other forces have met limitations.

The Detective Chief Superintendent of Economic Crime explained that there was a very large volume of targets – approximately 190,000. He explained that the CoLP are leading the world with regards to taking down criminal/fraudulent websites, and there was a strong desire to maintain its footprint beyond the limits of the City of London. He explained that a recent appearance on *Crimewatch* boosted the CoLP's profile. The Chairman explained that *Crimewatch* had recently been cancelled, and suggested that perhaps it would be beneficial for the Police Committee to write a letter to the BBC to show their support of its continued production.

The Detective Chief Superintendent of Economic Crime explained that there had been successful promotional work achieved across social media. The Chairman noted that the summary of engagement levels on social media, as referenced within paragraph 3.2, would benefit from more background information to supplement it. (3)

The Detective Chief Superintendent of Economic Crime explained that the 7% of victim respondents that were not satisfied with the service, could generally be attributed to those who had not received the outcome they had hoped for. He explained that this was always going to pose a challenge, regardless of

service standards, due to the volume of individual cases that don't result in positive outcomes. A Member suggested that it might be useful to alter the question in order to accurately portray the opinions of those with regards to the provision of victim care specifically. The Detective Chief Superintendent of Economic Crime agreed. (4)

The Detective Chief Superintendent of Economic Crime proposed that the layout of the reports submitted to the Board be changed to reflect the four priorities: Pursue, Protect, Prepare and Victim Service. The Chairman stated that the reports should be submitted in any format that is determined to be the most effective and useful, and approved this change.

The Detective Chief Superintendent of Economic Crime explained that there were currently 4 vacancies, and a Member asked what percentage of the total staff this amounted to. It was explained that this was 4 out of a total 23 positions. The Chairman noted that this seemed to be an urgent matter. A Member asked if there had been any useful Deloitte recommendations in this area, to which the Detective Chief Superintendent of Economic Crime confirmed that there were, and also stated that there needed to be awareness of the value in seeking external resources to cover costs rather than circulating costs within the City Corporation.

The Chairman noted an error in paragraph 5.3, where it stated there had been an increase of 56% in survey respondents. The figures included within the report illustrate that this was in fact a decrease of 36% from the previous period.

A Member queried the correspondence between the data in the "Total Outcomes Recorded" graph, and the following tables within the report, citing the total of approximately 11,000 Total Outcomes recorded in Q2 within the graph. Members discussed the use of cumulative recording of data, and all agreed that it would be best to refrain from using this method in the future when reporting ECD data. (5)

A Member asked for results-based evidence of progress made in these areas. The Detective Chief Superintendent of Economic Crime explained that they had shown improvements by reducing the number of KPI areas marked as RED down to just one, illustrating significant improvement.

A Member queried the root cause of the small number of final outcomes from total investigations. The Detective Chief Superintendent of Economic Crime explained that they were commencing new cases immediately as previous cases are finished, and due to lack of information in many instances these cases were not marked as "complete".

A Member queried the absence of data under the heading for "Value for Money". The Detective Chief Superintendent of Economic Crime confirmed that this would be available at the next meeting.

RESOLVED – That the report be noted.

7. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**
The Board received a report of the Commissioner of Police providing an update on the Economic Crime Victim Care Unit.

RESOLVED – That the report be received.

8. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no questions.

9. **EXCLUSION OF THE PUBLIC**

10. **NON-PUBLIC MINUTES**
The Board considered the minutes from the last meeting, held on 27 July 2017.

RESOLVED – That the minutes be approved.

11. **RESTRICTED ACTIVITY UPDATE**
The Board received a report of the Commissioner of Police that summarised notable Policing activity not for publication that is being delivered by the City of London Police in its capacity as the National Lead Force.

RESOLVED – That the report be received.

12. **ECONOMIC CRIME ACADEMY UPDATE**
The Board received a report of the Commissioner of Police updating Members on the developments of the Economic Crime Academy.

RESOLVED – That the report be noted.

13. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no questions.

14. **ANY OTHER NON-PUBLIC BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**
There was no further business.

The meeting closed at 12.17 pm

Chairman

Contact Officer: George Fraser
tel. no.: 020 7332 1174
george.fraser@cityoflondon.gov.uk

This page is intentionally left blank

POLICE COMMITTEE

2 November 2017

OUTSTANDING REFERENCES

No.	Meeting Date & Reference	Action	Owner	Status
1.	**21/09/17** Item 3a – *Minutes* Equality & Diversity Lead	A Member asked when the new CoLP lead for Equality and Diversity would be appointed. The Assistant Commissioner stated that it had been advertised and if no one applied then he would post someone in there at SWP on 22 September. The Assistant Commissioner would update Members on any progress. **UPDATE**: There have been 2 applicants in response to the advert for the post and interviews are in the process of being planned. It is estimated that with vetting, the successful applicant will be in post by December.	CoLP	**OUTSTANDING**
2.	**21/09/17** Item 3b – *Outstanding References* Use of colour within Agenda graphics	The Chairman mentioned that this was an issue in later items within the agenda, such as items 5 & 8, in which graphs that had been designed to be viewed in colour were rendered ineffective. He requested that this issue be addressed, either by the production of packs in colour, or through the production of graphs with monochromatic printing in mind. **UPDATE:** All CoLP reports will be double checked going forward and graphical data will be presented in monochrome / pattern as appropriate or RAG status shown in words. This has already been completed for the ECB Q2 Performance report**.**	CoLP/ Town Clerk	**ONGOING**

No.	Meeting Date & Reference	Action	Owner	Status
3.	**13/07/17** Item 8 – *Risk Register Update* Police Accommodation Monthly Update	It was agreed that there needed to be a separate monthly update on the Police Accommodation programme progress. There would also be a standing item on the Committee agenda	PAP Programme Director – Simon Rilot	**ONGOING –** Last update circulated to Members on 23/10/17
4.	**13/07/17** Item 25a – *Provision of a Uniform Managed Service for City of London Police Stages 1&2 Report* **21/09/17** Item 3b – *Outstanding References* Source of Clothing Stock	Members' questioned the source of the clothing stock. The City Surveyor agreed to provide this information to Members. A Member requested that there needed to be an overview of all procurement. The Chamberlain explained that there was a robust and substantial strategy in place, and agreed to send this to the Member.	City Procurement/ Chamberlain	**COMPLETE -** Information from City Procurement circulated to Members on 09/10/17
5.	**21/09/17** Item 4 – *Staff Survey* Staff Survey Final Report	The Chairman illustrated his approval of the Force's swiftness in bringing the initial Staff Survey report to Committee, and his desire to see the final report at Committee. The Assistant Commissioner agreed that the final report would be submitted to the December meeting.	CoLP	**REPORT DUE DECEMBER 2017**

No.	Meeting Date & Reference	Action	Owner	Status
6.	**21/09/17** Item 5 – *Annual Update on the Custody of Vulnerable Persons* Accommodation of Young People in custody	The Chairman requested feedback on the status of the recovery of the costs of accommodating young people in Police custody overnight when local accommodation could not be provided. **UPDATE**: The Custody Manager has confirmed that she has recovered all outstanding costs to date and none are outstanding.	CoLP	**COMPLETE**
7.	**21/09/17** Item 5 – *Annual Update on the Custody of Vulnerable Persons* Detainee figures contradiction	A Member asked for further clarification of the figures for number of detainees as represented in Appendix 3, suggesting that they were in contradiction to those portrayed in the ADR. (For 2016-17, Appendix 3 fig 11 showed approx. 28/29 persons MH initial assessment detained. Whereas ADR App 4 shows 167 detained under s136 MH act) **UPDATE**: The data as detailed at Appendix 3 is for people that have been arrested for an offence and then whilst in police custody display mental health issues and are then assessed and it is decided if they need to go to hospital (sectioned) for mental health assessment. The data detailed in the section in App 4, relates to people who are stopped/attended to on the street that do not enter custody. These are assessed by staff on the street with the street triage team and it is decided on the street if they need to go to hospital for a mental health assessment (detained sec 136).	CoLP	**COMPLETE**

No.	Meeting Date & Reference	Action	Owner	Status
8.	**21/09/17** Item 5 – *Annual Update on the Custody of Vulnerable Persons* The Concordat for Children in Custody	A Member requested confirmation that the City of London Corporation had signed The Concordat for Children in Custody. The Town Clerk agreed to follow this up. **UPDATE**: The Corporation is not signed up as there are issues within the concordat which are currently being addressed by the Association of London Directors Children Services and the Home Office. At this time, no London Local Authority is signed up.	Town Clerk	**ONGOING –** Update circulated to Members on 25/10/17
9.	**21/09/17** Item 5 – *Annual Update on the Custody of Vulnerable Persons* Use of Tasers on Under-18s	A Member requested information on the use of Tasers on under-18s, and how this was being recorded. The Assistant Commissioner explained that this was not covered by the report, but would source an update for Members. **UPDATE**: For the F/Y 2016-17 for U18, there was one use of TASER where the individual, a 16 year old, was 'red dotted'[1] (but TASER was not discharged). For F/Y 2017 to date there have been no instances of use of TASER on U18 year olds.	CoLP	**COMPLETE**

[1] Red dotted is when the TASER is drawn and aimed at a person and a laser light red dot appears on the individual so that they know that they are subject to the aim and can see the red dot on their person. Verbal warnings from the officer also accompany this. Depending on the reaction of the individual and the dynamic risk assessment of the officer, the officer will then use their professional discretion to decide whether to discharge the TASER or not. In this instance the TASER was not discharged. It is normally only drawn when there is a violent individual and there is an imminent threat to officer safety and/or a threat to the public.

No.	Meeting Date & Reference	Action	Owner	Status
10.	**21/09/17** Item 5 – *Annual Update on the Custody of Vulnerable Persons* Street Triage funding	A Member asked where the funding for the "street triage" system that was being piloted would be sourced from. The Commissioner agreed to follow this up and report back to Members. **UPDATE**: CoLP has funding for the MH Street Triage until May 2018 from the NHS East London Foundation Trust. There is a meeting in November with the City of London Corporation to discuss how this will be funded after May 2018.	CoLP	**COMPLETE**
11.	**21/09/17** Item 5 – *Annual Update on the Custody of Vulnerable Persons* Flowchart of Custody Procedure for Young People	The Chairman noted that the graph in Appendix 1 was incomplete, with an arrow leading off the printed area, and asked if this could be clarified.	CoLP	**COMPLETE -** A corrected version circulated to Members on 12/10/17
12.	**21/09/17** Item 6 – *Quarterly Community Engagement Update* Street Triage Pilot Outcomes	The Chairman requested that Members receive feedback of the results of the street triage scheme for which evaluation is due to be completed at the end of September, as referenced in paragraph 2.4 and 2.5 of the report.	CoLP	**COMPLETE -** Update circulated to Members on 24/10/17.

No.	Meeting Date & Reference	Action	Owner	Status
13.	**21/09/17** Item 8 – *Revenue Budget Monitoring Report to June 2017* ECD Funded Units expenditure	The Deputy Chairman queried one of the figures in Table 1, under the column for Q1 Actual, referring to the expenditure for ECD – Funded Units. **UPDATE**: The £18.32m figure in the Q1 Budget Monitoring Report is not a typo and the ledger is accurate. The ledger is showing debtor balances relating to grant funding which had not been paid – hence it is in the ledger as a debit balance. When the grant is paid it clears the debit by crediting the balance. At quarter one the grants outstanding across the units were unpaid hence the large debit balance.	CoLP	**COMPLETE**
14.	**18/05/17** (1) Barbican CCTV	CCTV upgrade The Commissioner advised that further work was being undertaken on the scoping of Phase 2 of CCTV upgrade and, owing to Crossrail and major building developments in that area, a report would not be expected until May 2018.	CoLP / Safer City Partnership	**Report due May 2018**

Committee:	**Date:**
Police Committee – For Information	2nd November 2017
Subject Health and Safety Annual Performance Update 1st April 2016- 31st March 2017	**Public**
Report of: Commissioner of Police Pol 66-17	**For Information**

Summary

This report provides information on the current position regarding the management of health and safety within the City of London Police (CoLP) since the last report submitted in September 2016, Pol 39-16.

Progress against the Force's action plan has continued and a safety maturity matrix has been created to support progression of safety risk management within CoLP. The existing action plan has been updated to include milestones that will support the Force as it advances its safety maturity. Progress and the introduction of new milestones will be incorporated into the action plan which runs for the period October 2017 to September 2020 for Members information the Force Action Plan 2014 – 2017 is attached at Appendix 1, the additional actions which will be added to this plan to cover the period 2017 -2020 are attached at Appendix 2.

Initial actions, which form key milestones, have been identified to support the introduction of this model including running a health and safety leadership workshop for senior managers within CoLP in line with recent mandatory requirements at the City of London Corporation. Other actions include health and safety training for managers and the introduction of an electronic accident and near miss reporting system.

Management of the Force's Top X risks continues, and in line with the Corporate Top X management process, during the course of the year risks that were escalated to the Force register have been mitigated to an acceptable level and subsequently removed from the Force register.

Wellbeing of employees is a growing area of importance for many organisations and is often linked with health and safety. The City of London Corporation has adopted this approach, and, during the course of this reporting year, the Force has extended the remit of the Force Health and Safety Committee to include Wellbeing. In addition, and in recognition of the growing importance of employee wellbeing the Force has appointed a Wellbeing Champion who is a Senior Leadership Team member and can provide a strategic link between the Senior Leadership Team and the network of health and wellbeing volunteers.

RECOMMENDATIONS

It is recommended that Members receive and note the contents of this report.

MAIN REPORT

Background

1. The City of London Police (CoLP) submits a report annually to your Committee on the progress made in applying Health and Safety policy and practice, and advises Members of any developments during the year.

2. The period covered by this report is from 1 April 2016 to 31 March 2017, although up-to-date information in some areas is provided for Members information.

Current Position

3. During the course of the past year changes have been made to the structure of the Force Health and Safety Committee. The membership of the committee has been extended to include the Force's Wellbeing Champion, a role that was introduced into the Force in early 2017. It is anticipated that the Wellbeing Champion will provide a strategic link between the health and wellbeing network of volunteers and the Force Health, Safety and Wellbeing Committee.

4. The Committee will continue to monitor the progression and effectiveness of the management of health and safety across the Force.

5. A wellbeing action plan was developed early in 2017 and the implementation of this action plan will be monitored at the Force Health, Safety and Wellbeing meeting.

6. The Force has a Health and Safety Action Plan which has been in place since 2014. The plan has been reviewed and amended to cover the period October 2017 – September 2020. It incorporates changes to support the progression of the Force's safety maturity model.

7. As is common in many industries, including other Police Forces, a health and safety maturity matrix has been developed and outlines the criteria needed to demonstrate various levels of safety maturity. It is based upon best practice from various industry sectors and, in particular, other Police Forces such as the Metropolitan Police Service.

8. According to the Health and Safety Executive (HSE) the use of such maturity models reflects an organisation's degree of readiness to tackle safety risks.

9. The maturity matrix will be used to progress safety cultural maturity within City of London Police; it will be used to provide a framework for development. A number of milestones are being incorporated into the

Force Action Plan to progress safety culture over the coming 3 years. However, full progress will take longer than 3 years and actions will be needed to continue this work beyond September 2020.

10. In addition, over the coming year work needs to be undertaken to thoroughly understand the health and safety risk profile of individual teams and directorate.

11. This will feed the Force-wide strategic, health and safety risk profile. This in turn will inform processes such as policy and guidance development, Top X and audit and assurance requirements.

12. This will be time consuming and will create a significant impact upon the workload of the Force's dedicated Health and Safety resource which consists of one person.

13. The Force Health and Safety Action Plan is designed to support Directorates in their management of health and safety. It reinforces the mechanism to escalate issues which cannot be resolved locally, or which have Force-wide implications, to the Force Health and Safety Committee and onward to Force Risk Assurance Group or the Corporation of London Corporate Health, Safety and Wellbeing Committee if deemed necessary.

14. The format of the current action plan will form the basis for the Force Health and Safety Action Plan for the period 2017-2020. However, it will be updated as the risk profiling work is undertaken to reflect the actions needed to progress the organisation's safety maturity. The additional actions are attached at Appendix 2 for members' information.

15. Oversight of the progression of the actions identified on the Action Plan will continue to be monitored by the Force Health, Safety and Wellbeing Committee.

Wellbeing

16. As described in the report to your committee in September 2016 the Force, through a network of volunteers, has set up a Health and Wellbeing network.

17. Earlier this year a Wellbeing Champion, who is part of the Force's Senior Leadership Team, was appointed.

18. The Wellbeing Champion will provide the strategic link between the voluntary Health and Wellbeing Network to Board meetings such as the Senior Leadership Team and Force Health, Safety and Wellbeing Committee.

19. To reflect the changes that are taking place regarding the importance of the wellbeing of staff and officers the Force's Health and Safety Committee now incorporates the strategic governance for wellbeing.

20. In recognition of this committee has been renamed the Force Health, Safety and Wellbeing Committee.

21. The Wellbeing Champion attends these meetings and provides an update on progress of wellbeing initiatives being ran in Force. Over time, it is anticipated that the effectiveness of these initiatives will be monitored at the Force Health, Safety and Wellbeing Committee.

Risk Management

22. Top X is the process for considering the top health and safety risks across the Force.

23. Formal reviews are held at the Force Health, Safety and Wellbeing Committee meetings on a quarterly basis. However, directorates are encouraged to amend their directorate level Top X registers as and when necessary, for example with the emergence of new risks.

24. These can then be monitored at directorate level and escalated to the Force Top X register.

25. For Members information the Force's current Top X risks are:

Custody – Training for some Custody Sergeants requires updating. Urgent training has been arranged and temporary measures initiated until a sufficient number of custody-trained sergeants skills have been updated. In addition, during November additional officers will attend custody sergeant training courses to provide further resilience.

- **Body Armour** – where delays were being experienced, for a number of reasons, in obtaining body armour. New processes have been introduced to reduce the time taken for new recruits to be measured up for their body armour and it is anticipated that this risk will be removed from the Force Top X register at the next meeting of the Force Health, Safety and Wellbeing Committee but will continue to be monitored at Directorate level and escalated if deemed necessary.

- **Fire safety** – Fire risk assessments for CoLP occupied buildings have recently been undertaken and some areas for improvement have been identified and passed to the Force's Facilities Management Team for consideration, where applicable, with the City Surveyors Department.

  Training for all fire marshals is taking place during September. The arrangements for invacuations at all CoLP occupied buildings are being to be agreed between the Facilties Management Team and Information and Intelligence Directorate representatives who will organise

invacuation drills once finalised. Fire Safety will remain on the Force's Top X register for monitoring purposes until all actions are complete.

Force gyms – the need for controls around who can use the on-site Force gyms and actions related to this such as health checks and gym inductions and lone gym users have been identified as an area where some work is needed to mitigate identified risks. Progress is being made on the other areas where work is needs to be undertaken are being finalised such as who will deliver the gym inductions, access control doors and wall phones to summons help. Once agreement has been agreed a guidance document to support these processes and those delivering them will be produced.

Accident and Incident Reporting

26. Over the past 3 years the numbers of accidents and near miss reports have continually increased. During the 2016/17 reporting year it is noted that the number of reports of injury have gone down but the number of near misses has significantly increased.

27. A number of near miss reports (23) were raised in relation to vulnerability of Police Officers due to staffing levels on response teams.

28. The minimum strength numbers of response teams will be managed by the Assistant Commissioner and Commander Operations and Security at Senior Leadership Team level.

29. Other actions have been taken to address this including aligning Special Constables to bolster numbers, giving Inspectors the authority to backfill from Officers undertaking office duties.

30. There are no other specific trends related to the number of near miss reports.

31. The increase may be due to on-going promotion such as including accident and near miss reporting as part of the induction programme for new entrants to the City of London Police during the past year. This is in addition to ongoing promotion at Force and directorate level, of the importance of reporting accidents and near misses. Table 1, - Accident and Incident Data refers.

Table 1 – Accident and Incident Data

Totals	2014-2015	2015-2016	2016-2017
Police Officer	38	51	42
Police Staff	8	5	7
Others (including Agency workers, contractors and detainees)	3	4	4

Accident totals	49	60	53
Near Miss Totals	9	16	41
RIDDOR	2	4	3

32. During the reporting period the RIDDOR[1] reports to the Health and Safety Executive (HSE) comprised of one Police Officer who sustained a lower back injury following a bicycle training course this is classed as an 'over 7 day injury'. This type of incident becomes reportable where an employee is absent from work, or at work but unable to undertake their normal duties due to an injury at work for 7 consecutive days or more. The second involved a Police Officer who sustained a broken ankle whilst giving chase and the subsequent arrest of a suspect. The third reportable incident occurred when a member of the contract cleaning team broke a bone in her foot when something fell out of a cupboard causing the injury.

33. The HSE continue to carry out an investigation which is currently still live. Members should refer to the Non-Public Restricted Appendix 3 for further detail on this.

34. As reported last year the Force was looking into the possibility of moving it's accident and near miss reporting system to that which is used in other departments of the Corporation of London.

35. As a contingency measure, because this system is not used by any other Police Forces, other options to move CoLP from a paper-based accident and near miss reporting system were being considered. And, preliminary investigations into systems used by other Police Forces were being undertaken.

36. Following these investigations, it has been decide to incorporate the accident and near miss reporting system as a module on the HR/Origin system.

37. This will provide benefits in the collation and sharing of information within Force.

38. The introduction of the accident and near miss reporting modules is being progressed as part of the Integrated HR System Upgrade Programme.

[1] RIDDOR: the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013. Reportable incidents include fatalities to workers and non-workers, major injuries from a prescribed list including amputations, fractures (other than to fingers, thumbs and toes) and asphyxia. All workplace injuries that result in a worker being either absent from work, or, unable to undertake their normal duties for seven consecutive days or more. Non fatal accidents to non-workers where the non-worker is taken directly to hospital. Certain, specified occupational diseases. Dangerous occurrences from a list of 27 such as: the collapse, overturning or failure of load-bearing parts of lifts and lifting equipment.

39. The target implementation date is June 2018.

Force Health and Safety Action Plan 2014 – 2017

40. The current Force Health and Safety action plan commenced in November 2014, it is designed to support Directorates to manage risks locally and provide a defined escalation process for those risks which cannot be managed locally or have Force-wide implications. For members information a copy of the Action Plan is attached at Appendix 1.

41. There are 12 actions in the current Force Action Plan and each Directorate has an individual action plan which is aligned to individual, Directorate risks.

42. For members information table 2 below, provides an overview of the RAG status of actions over the past year.

Table 2 – Overview of Force Action Plan RAG Status

Number of actions currently rated as:	August 16	November 16	March 17	June 17
Red	0	0	1	0
Amber	6	7	5	4
Green	6	5	6	8
Total number of actions:	12	12	12	12

43. Five of the amber actions where further work is required relate to Planning and Arrangements whilst the remaining action relates to implementation. Progress on these actions appears to have slowed due to the Force restructure which ran into the beginning of 2016, and, over the past year progress has resumed.

44. These actions are being progressed and their status will be reviewed at the next Force Health and Safety Committee in October.

45. The action plan will be amended to cover the period October 2017 – September 2020 and will include the milestones identified to drive progression against the maturity matrix.

Training

46. The Force has an Induction Day Training course for all new entrants to City of London Police. This induction day includes a presentation on health and safety including information such as the importance of accidents and near miss reporting.

47. The Force is working to introduce a Management Development Programme. As part of this course there will be specific health and safety modules for managers on their responsibilities. It will include a separate in-depth session on risk assessments.

48. It is anticipated that the health and safety modules will be introduced in April 2018.

49. A health and safety leadership workshop will be run in City of London Police once work to scope out the Force's requirements has been completed. This is in line with recent changes to Corporation of London Mandatory Health and Safety training for senior management in all Chief Officer Teams.

50. Training is a key component to manage risks and being able to access individual training records is important for monitoring purposes. Improvements are being introduced to centralise driver and rider training including IT solutions to accurately record essential training.

51. The Learning & Development Team have introduced measures to increase output and rationalise the recording of driver records to become fully compliant with national Police standards.

Assurance

52. Each Department of the City of London Corporation is required to complete an Annual Certificate of Assurance covering the period 1st January – 31st December annually. The purpose of the report from Department Directors/Chief Officers to the Town Clerk is to provide assurance that the department has a health and safety management system and an assurance process.

53. In line with the Force's Top X risks, in particular, Fire Safety, improvements in the management of fire safety were identified.

54. Although CoLP is compliant with this assurance process. The provision of a more in-depth internal assurance and auditing programme by the Force's Head of Health and Safety continues to prove challenging due to workload demands.

55. Preliminary investigations into the viability of electronic systems which are used in other Police Forces to support the management of audits and assurance is currently being undertaken.

Recommendations

It is recommended that Members receive and note the contents of this report

Conclusion

56. Progress against the Force's action plan has continued and the existing plan has been updated to include milestone that will support the Force as it progresses its safety maturity.

57. Actions have been identified to support the introduction of this model including training for managers and a health and safety leadership workshop for Senior Managers within CoLP, in line with Corporation of London requirements. The introduction of an electronic accident and near miss reporting system and health and safety training modules for managers form other key milestones.

58. Management of the Force's Top X risks continues. In line with the Corporation of London's Top X management process, during the course of the year risks that were escalated to the Force register have been mitigated to an acceptable level and subsequently removed from the Force register although they will continue to be monitored at directorate level.

Contact:

Nicola Scoon
Head of Health and Safety
Tel: 020 7601 2288
E-mail: nicola.scoon@city-of-london.pnn.police.uk

This page is intentionally left blank

City of London Police Health and Safety Action Plan 2014 -2017

Planning and arrangements								
Area of Focus	**Who is responsible for delivery?**	**How will this be measured/expected outcomes?**	**Due by:**	**Evidenced by:**	**RAG status and update as of Aug 16**	**RAG status update as of Nov 16**	**RAG status update as of March 17**	**RAG status update as of June 17**
The Force has an up-to-date H&S Policy authorised by the Commissioner	**HoH&S**	**Policy is accessible to all on intranet. Responsibilities and understanding of policy will be tested at all levels as part of assurance programme**	**Policy updated and in place by January 2015, this will be published and disseminated for implementation. Assurance checks will be on-going and results presented to quarterly Directorate and Force H&S Committees**	**Up-to-date policy exists and is accessible to all on intranet**	**GREEN Policy up to date update policy statement from Commissioner to be added**	**GREEN In progress**	**GREEN**	**GREEN Policy details up to date, new statement from Commissioner.**
The Force has a framework of H&S SOPs and guidance to support the overarching H&S policy implementation	**HoH&S**	**SOPs and guidance available on intranet. Ongoing review of SOP and Guidance documents. Review timetable will be presented to Force H&S Committee**	**Timetable of updates will be included as/when presented to Force H&S Committee. This will be continuous over the 3-years of the plan Planned SOPs**	**Updated SOPs will be available to all on the intranet**	**AMBER The review of existing SOPs will take longer than originally planned. This work was originally planned due to unforeseen**	**AMBER As previous comment**	**AMBER New Accident Reporting SOP and Accident Investigation guidance new SOPs and Guidance**	**GREEN Accident and Near Miss reporting updated DSE Guidance documentation published PPE currently updated September 2017**

			and guidance up to March 2015 are: H&S Guidance to Support Lone Working Policy H&S Guidance to Support Agile Working Accident and Incident Reporting SOP in line with introduction on new reporting system		resourcing issues		added	
Directorates demonstrate planning of their own H&S arrangements	Directorate Heads	Up-to-date H&S policy endorsed by current Head of Directorate Where a Directorate leads on a specific area, and, as dictated by risks encountered the lead Directorate will produce health and safety guidance for the Directorate and Force. Minutes of	Review dates as part of a rolling programme in-line with quarterly H&S Directorate and Force H&S meetings which will be continually updated	Documentary evidence will be available	AMBER As per previous comments. Progress is now being seen and it is anticipated that this action will be Green by November	AMBER Due to changes in management arrangements in some of the directorates this action is still shown as Amber	AMBER As per November comments	AMBER but imminently GREEN Anticipated this action will be up-to-date after latest round of directorate meetings and will be turned green

		meetings where planning including H&S considerations is considered are recorded						
For operational and/or project work Directorates are able to demonstrate they consider health and safety implications	Project leads	Documented evidence including; project plans, minutes of meetings and action plans.	Rolling programme of quarterly reviews in-line with H&S Committee meetings	Documentary evidence will be available	GREEN As per comments at May	AMBER Due to management arrangements for H&S in some directorates documentation has not been provided. Work is ongoing to address this with the relevant directorates	AMBER As per November comments	GREEN Document checks are included in audit/inspection programme to provide assurance
Emergency planning. Directorates are able to demonstrate they adhere to the Force's emergency planning arrangements. In particular ensuring that there are	Directorate Heads General Services Director	Evacuation Marshals details are easily identifiable to all and each Directorate has enough Evacuation Marshals to cover the areas they work in	Review in line with Force H&S meetings	Up-to-date lists of Evacuation Marshalls readily available and published on intranet	AMBER Arrangements for fire evacuation points are being drawn up by FM Team and will be agreed with SB. Other	AMBER Although there has been a lot of progress regarding appointment of fire marshals some areas still do not have fire marshals – building list	AMBER Awaiting decision on Invacuations	AMBER Improved, once the latest round of directorate meetings have taken place it is anticipated this action will be on track. Fire marshals list circulated to H&S SPOCs for updates

sufficient numbers of Evacuation Marshals to cover the areas that their teams work in and that they work in collaboration with Facilities Managers					**arrangements (such as notification of evac points have been agreed) and will be implemented once agreement from SB has been obtained.** **Drills of both invac and evac to take place at all buildings within next 3 months.** **New CoL Fire Safety Policy has been produced and provides clarity on responsibilities however, some areas within CoLP require agreement, as arrangements at CoLP for a 24/7 estate**	**circulated to directorate H&S SPOCs for completion by 15 November** **Training will be arranged once this has been done**		

					need to be addressed. For discussion at Force H&S Committee in Augus			
Area of Focus	**Who is responsible for delivery?**	**How will this be measured/expected outcomes?**	**Due by:**	**Evidenced by:**	**RAG status and update Aug 16**	**RAG status and update November 16**	**RAG status and update March 2017**	**RAG status and update June 2017**
Do all Directorates have risk registers which are maintained and up-to-date?	Directorate Heads	Risk Registers are available upon request and are up-to-date. Directorate risk registers will be reviewed as part of individual Directorate Health and Safety meetings.	Quarterly milestones in line with Directorate H&S Committee meetings	Up-to-date Directorate risk registers Minutes of Directorate H&S meeting.	AMBER With formation of new BS Directorate arrangements are currently under review it is anticipated that details and arrangements are in place by November 16 status will be turned back to Green	AMBER As per August update however, November target has not been met	RED As per August and November	GREEN Improved situation, RR now being updated however work needed across all directorates to ensure this action is fully up to date
Do all Directorates have asset registers which are up-to-date and detail equipment that	Directorate Heads	Asset register of equipment subject to regular safety checks and maintenance is available and gives details of:	Quarterly reviews will be undertaken in line with individual directorate H&S Committee	Directorate registers are up-to-date and available upon request. Minutes of Directorate	AMBER As per May's comments verbal update to be given at Force H&S	AMBER As per August update	AMBER Appear to be problems where the directorate pages have	AMBER HR self service has a module where information can be loaded. Currently under investigation

require regular safety checks and maintenance? Does each Directorate have a testing and maintenance schedule?		schedule for planned maintenance checks along with any comments necessary, dates of scheduled testing and calibration along with results of test.	meetings. Findings will be monitored at Force H&S Committee meetings	and Force H&S meetings are available to demonstrate management reviews of findings along with corrective actions if required	meeting in August		been moved and are no longer aparant. This is being looked into by directorates	by HoH&S as this may provide a more effective management tool and prompt for those who have equipment subject to testing
Area of Focus	Who is responsible for delivery?	How will this be measured/expected outcomes?	Due by:	Evidenced by:	RAG status and update August 2016	RAG status and update November 2016	RAG status and update March 2017	RAG status and update June 2017
All Directorates are able to demonstrate that they undertake pro-active monitoring of their activities and take timely, effective actions to address emerging issues, and that they periodically test	Directorate Heads	Minutes of meetings including Directorate H&S, minutes of planning and where appropriate debriefing meetings Any documentation relating to changes that have been implemented as a result of pro-active monitoring. At Force level: Accident and Incident data monitoring	Quarterly reviews in-line with Directorate and Force H&S Committee meetings	Documents including minutes of Directorate H&S meetings, operational planning and de-briefing information. Sickness Data Monitoring by PMG monthly	GREEN Directorate H&S meetings held as follows: CI: 19/7/16 BSD: - future plans for H&S arrangements discussed at BSD SMT meeting 9/8/16 ECD: 13/7/16 I&I: 12/8/16	AMBER Not all directorates have held meetings this quarter however H&S is discussed at BSD SLT	AMBER As per previous comments	AMBER Improved situation anticipated that this action will be up-to-date after latest round of directorate meetings

Page 351

the effectiveness of their risk control measures		sickness data monitoring for trends			UPD: 2/8/16			
Area of Focus	**Who is responsible for delivery?**	**How will this be measured/expected outcomes?**	**Due by:**	**Evidenced by:**	**RAG status and update August 2016**	**RAG status and update November 2016**	**RAG status and update March 2017**	**RAG status and update June 2017**
All Directorates are able to demonstrate that they undertake re-active monitoring and take appropriate actions to prevent reoccurrences	Directorate Heads	Minutes of meetings Details of management follow up and corrective actions following accidents and incidents	Quarterly reviews in-line with Directorate H&S meetings	Documents including Directorate H&S Committee meetings, accident and incident investigation reports, Force level – minutes of Force H&S meetings	GREEN As comments above re directorate meetings and changes further investigations discussed for example review of accident and near miss stats	GREEN As per August comments	GREEN	GREEN
The Force has an Assurance and dip-sampling programme	HoH&S	Results of assurance checks and dip-sampling	Rolling schedule – schedule to be drawn up	Reports to Directorate Heads, Force Health and Safety Committee and other appropriate persons, as deemed necessary, are available	GREEN Dip sampling and assurance programme under development	GREEN Annual certificate of assurance completion is currently being undertaken	GREEN Annual certificate of assurance completed based upon self-assessment	GREEN Schedule for directorate inspections published, assurance checks of Building Manager monthly checks will be undertaken and specific

				upon request				inspections/audits to take place during the next quarter details will be fed back to relevant managers and Force H, S & W committee
Area of Focus	**Who is responsible for delivery?**	**How will this be measured/expected outcomes?**	**Due by:**	**Evidenced by:**	**RAG status and update August 2016**	**RAG status and update November 2016**	**RAG status and update March 2017**	**RAG status and update June 2017**
All Directorates are able to demonstrate regular senior management review of H&S performance	**Directorate Heads**	**Departmental escalation mechanism for H&S issues exists: Directorate H&S meetings are held quarterly and are attended by all Heads of Departments and chaired by Directorate Heads or other senior manager within Directorate High level review of departmental H&S performance takes place on a regular basis - evidenced by minutes of SMT**	**Quarterly dates of planned meetings to be added this will be populated in advance on an on-going basis**	**Minutes of Directorate H&S meetings are available Minutes of Directorate SMTs are available to demonstrate SMT H&S performance review and any actions taken**	**GREEN Over the past quarter directorates have held H&S meetings at which managers discuss their directorates H&S performance**	**GREEN As per August comments**	**GREEN**	**GREEN**

		meetings						
The Force is able to demonstrate regular senior management review of H&S performance	Senior management at Chief Officer Group level	Force escalation mechanism for H&S issues exists from Directorate level to Force H&S Committee HoH&S attends Risk Assurance Group meetings Scheduled H&S reporting to SMB Annual reporting to Grand Police Committee	On-going quarterly review in line with Force H&S Committee meetings:	Minutes of Force H&S meetings available Minutes of other senior management meetings where H&S is discussed available along with decisions and actions taken	GREEN SLT review of H&S takes place – the SLT approved the Force Annual H&S Performance report to Police Committee at their July meeting. All directorates held H&S meetings or discussed at length at relevant SMT	GREEN Health and Safety issues escalated to SLT as appropriate. Annual certificate of assurance will be reviewed by the SLT and signed off by The Commissioner	GREEN	GREEN

This page is intentionally left blank

Additional Actions for Force H&S Plan period 2017 - 2020

Area of Focus	Who is responsible for delivery?	How will this be measured/expected outcomes?	Due by:	Evidenced by:	RAG status update as of	RAG status update as of	RAG status update as of	RAG status and update as of
H&S leadership training for SLT members. This is a mandatory Corporate requirement	**SLT L&D**	**Workshop arranged with Human Apps and all SLT members have attended**	**March 2018**	**All SLT members have attended the H&S Leadership workshop and cascaded key messages to their teams**	**New item for 2017-20**			
Local management of DSE assessments and compliance	**Directorate Heads**	**There is a monitoring and follow up process for the management of DSE assessments within directorates. Force-wide assurance checks to monitor**	**Directorates to establish system and requirement for training and assessments by January 2018**	**Systems that can be audited and assurance provided as a result**	**New item For 2017-20**			
Health and Safety training modules included in the Management Development training package	**L&D HoH&S**	**Managers receive class-room based training in their management responsibilities and risk assessment modules**	**March 2018**	**The quality of risk assessments, identification of the need for risk assessments** **Quality of management follow up following accidents and near misses**	**New item for 2017-20**			

Proposed changes to processes, people and policies and guidance have considered the health and safety implications	**Stage 1 – HoH&S**	**Stage 1 – identify the level and type of changes and how the consideration of health and safety can be evidenced**	**January 2018**	**Proposal for how decision making for changes to process, people, policies and guidance will be evidenced**				

Committee(s):		Date(s):
Police Committee	For Decision	2nd November 2017
Subject: City of London Police IT Strategy		**Public**
Report of: The Chamberlain and Commissioner of Police Pol 71-17		**For Decision**
Report Author: Sean Green, IT Director		

Summary

This attached City of London Police IT Strategy sets out the proposed strategic direction for City of London Police IT Service over the next 3 years, up to 2020.

The CoLP IT Strategy has been endorsed by the IT Sub-Committee, Finance Committee and the Commissioner's Strategic Management Board on the 11th October 2017.

Recommendation(s)

Members are asked to:

- Review and agree the attached CoLP IT Strategy.

Main Report

Background

1. This strategy builds on the work around core principles for the IT service, which are summarised below;

    - Buy-not-build.
    - Use fewer systems more effectively.
    - Secure and compliant IT systems and services that support the
    - organisation.
    - Move from complexity to commodity.

2. The aim of the strategy is to define in more detail the route map to establishing a modern fit for purpose IT environment that supports the effective delivery of the City of London Police business. At this stage it is very much about "getting the basics right."

3. At the core of the IT Strategy is the context around the current important IT infrastructure transformation projects, and the additional schemes that will

need to be progressed in the medium term. It reflects a better understanding of legacy issues and the challenges that must be addressed to reduce the current IT risk profile.

4. The City if London Police IT strategy has been developed in partnership with City Police colleagues, taking account of the national digital policing agenda.

5. The IT Strategies for the Corporation and the City of London Police have to be read in conjunction with the overall IT Strategy design principles attached as Appendix 1.

Current Position

6. The strategy aims to set out the current state of play, what we can learn from the past and how we can shape the future with a clearly defined strategy and road map. The upgraded environment will be a significant step forward in how the services are delivered and how end users can collaborate and work in the environment.

Context and Summary of Key Themes

7. The aim is to ensure that the underlying technology will enable rather than constrain the business. Following completion of both the Network and Desktop Transformation a summary of some of the key capabilities are set out below:

    - Performance
        - Log on speeds of sub 1 minute from power on
        - Replacement of oldest end-user hardware both laptops and desktops
    - Desktop Experience
        - Full Microsoft Office 2016 on all devices
        - Ability to use Instant Messaging and hold Video call from your device
        - Share your desktop and documents for collaboration
        - Ability to view Project and Visio documents
        - Applications deployed on demand directly to the device

- Connectivity
    - Ability to work from any location
    - Open your laptop and connect to the CoLP environment from any location with a secure internet connection with no additional tokens required
    - High bandwidth connectivity from all Corporate locations

8. This document is concerned with the technology strategy and not the Information and Application strategy which is a separate methodology linked to business strategy and business process. Contextually it is focused primarily on the hygiene factors that support the business and our users: Wide Area Network, Local Area Network, exploiting our Microsoft platform (Exchange and SharePoint) and the desktop experience.

Future Phases

9. It is anticipated that further iterations will expand on how the IT Division will aim to tackle other elements of the technology landscape, including new National Police technology programmes and digital services for the City of London Police.

Conclusion

10. IT is critical to business success and for the modern enterprise. It is essential that the underpinning IT and services are fit for purpose and support the goals of the organisation. It is appropriate at the technology level for both the City of London Police and the City of London Corporation to share a common approach and leverage the benefits of collaboration while recognising at the application and security layer both organisations have unique and separate requirements.

11. The common approach is based upon standardisation while recognising the programmes are implemented separately to deal with each respective organisation's uniqueness.

10. The CoLP IT strategy (attached as appendix 2) reflects the need to provide the framework in which our core IT components are managed and delivered. This is now demonstrated in the work undertaken by the IT Division on the technology stack review and work already underway on IT transformation planning and delivery for the new CoLP IT Networks.

Recommendation

11. Members are invited to comment and agree the approach set out.

Appendices

- Appendix 1 – IT Strategy Design Principles
- Appendix 2 - City of London Police IT Strategy
- Appendix 3 – City of London Police Security Policy

Sean Green
IT Director City of London Corporation and
City of London Police
Chamberlain's Department
T: 0207 332 3430
E: sean.green@cityoflondon.gov.uk

IT Transformation Programme

Appendix 1

City of London Corporation and City of London Police

IT Roadmap - 2020 Vision

Design Principles to Enable Business Collaboration

(Only to be read in conjunction with the CoL or CoLP IT Strategy Documents)
Approved by IT Sub Committee 22.2.2017
Review 22.2.2018

Document Details

Version	Modifications	Author	Date
0.1	First draft	Adrian Davey	15/02/2017
0.2	Second draft – Minor changes from proofing v 0.1	Adrian Davey	15/02/2017

Approvals

This document requires the following approvals:

Name	Role	Signature	Date	Version
Peter Kane	Chamberlain		15/02/2017	0.2
Sean Green	Director of IT		15/02/2017	0.2
Alistair Sutherland	Assistant Commissioner		15/02/2017	0.2
IT Sub Committee	Endorse		22/02/2017	0.2
Finance Sub Committee	Endorse		02/05/2017	0.2
Police IT Strategy Board	Endorse			0.2
Police Senior Management Board	Endorse			0.2
Police Committee	Endorse			0.2

Distribution

This document has been distributed to:

Name	Role	Date of Issue	Version
IT Transformation Steering Group		January 2017	
IT Steering Group		January 2017	
Police Strategic IT Board		February 2017	
IT Management team		February 2017	
Police IT Strategy Board	Endorse		0.2
Police Senior Management Board	Endorse		0.2

Contents

Introduction and Context

The City of London Corporation (CoL) and the City of London Police (CoLP) have a shared history and common values. While distinct organisations they both service the needs of the City of London. Through their community activities they also have a desire and need to collaborate and share information. Over many years this has led to the organisations becoming increasing integrated while maintaining their identities.

Integration has its challenges as both organisations have multiple stake holders both internally and at a national level, from National Police Federations through to local Government bodies. They also have differing requirements, particularly the Police which is a 24x7x365 operation referred to as a "blue light service" and security requirements due to the level of highly sensitive information.

The CoL and CoLP are now at a point where they need to re-evaluate both the demands they have for IT services and how those IT services will be supplied. The current Technology Stacks have reached both the end of their supportable life and end of serviceable life.

This challenge represents an opportunity to deliver a common approach to the Transformation of IT, to support the goal of current and future collaboration recognising a common approach with two distinct programmes.

This paper sets out the design principles that both organisations are following, to develop their respective IT Strategy and enable future collaboration.

In practical terms this is being demonstrated on the ground today with the upgrade of the network, which shares the common principles and approach but being implemented as two complimentary programmes.

IT Strategy and Enabling Collaboration

CoLP and CoL are consumers of IT and ultimately their strategy is based upon;

- The services they need to consume
- Market trends
- The transformation required to enable those services

At an infrastructure level both organisations need to consume;

1. A Wide Area Network to deliver bandwidth
2. A Local Area network to route traffic
3. A desk top for the end user
4. Collaboration software to support their organisations

It is these components that are the focus of the shared approach.

These components are the key to collaboration and by sharing common standards it will optimise the opportunities for future collaboration.

In principle the basic business requirements for the 4 components are identical as both organisations are subject to the same market trends and the same needs. At a practical level though they have different business models that require separate programmes.

This comes to the final point on the transformation required to enable these programmes particularly for the Police where early drafts would indicate a significant effort required from the front line Officers to adapt to the change.

Strategy is about shaping the future and has 3 components;

- Diagnosis: analysing the environment or situation, making a diagnosis
- Guiding Policy: setting the Policy framework
- Action Plans: sequencing the tasks and activities

The key point is strategy is not a vision but is the defined action plan based upon the Guiding Policy and the diagnosis of the current issues.

The diagnosis points to similar issues across both organisations at the IT level of technology infrastructure though at the application level the organisations vary considerably due to different demands. At a Policy level the Police are dictated by their security requirements. This is inevitably leading to similarity of requirements but with different programmes.

Given this both organisations are committed to developing a Strategy in partnership that recognises the opportunity for enhanced collaboration, follows the same process and methodology but is aligned to their individual organisation requirements.

Design Principles and Business requirements

Both Strategies are based on a set of core business requirements and design principles;

Design Principles

- Policy led design
- Remove complexity and simplify wherever possible
- Deliver end to end solutions
- Ensure the support model transforms in parallel with the technology
- Adaptable to current and future needs
- Alignment to industry trends
- The Technology Stack will be architected to best practice providing resilience and redundancy at all levels where cost effective and aligned to business requirements
- The Technology Stack will be designed to support the requirements for cost effective ICT services
- Cloud solutions wherever possible
- Technology Stack platform based around a single vendor where possible
- The Technology Stack will be maintained at the latest patch and release levels (n-1)
- The Technology Stack will be monitored and maintained at all times
- Compliant with regulatory frameworks (PSN, PSNP etc)
- The Technology Stack will be fully documented at all times
- Aligned to good industry practice and architectural principles
- Eliminate vendor device proliferation and collapse functionality into minimum number of devices

Core Business Requirements

- Enhance the end user experience
- Deliver a platform to enable a more mobile workforce
- Enhance the reliability and functionality of our environment
- Align the user experience to modern ways of working
- Deliver collaboration to provide a connected workforce
- Place CoL and CoLP into best in class for technology adoption and exploitation
- Provide our users with appropriate tools to do their jobs
- Align user expectation and user perception

IT Roadmap and The Enabling Collaboration Principles

To deliver the requirements for future collaboration both Strategies have a core alignment at the technology level for the 4 key components, sharing a common set of design principles. The LAN, WAN (referred to here as the network), desktop and collaboration software have been jointly articulated to share this approach.

Network

The current network comprising of the local and wide area network has reached end of life and cannot support future collaboration objectives. Consistent and repeatable failures are diminishing our ability to operate. Bandwidth constraints at multiple sites are failing to keep up with user demands.

The Transformation Programme envisages;

- To deliver an upgraded network for both the CoL and CoLP – both LAN and WAN
- Utilise a common standard for Network switches
- Utilise a common standard for Wide Area networking utilising the BT MPLS network
- Utilise common design principles and approach
- Support future mobile working practices with a corporate WiFi solution
- To enable future collaboration between CoL and CoLP and other parties
- Utilise a common High Level design

But to implement the network as two separate programmes to;

- Align the programmes to low level business requirements
- Align the network to the respective topologies and configuration requirements
- Ensure Corporation and Police security policies are adhered to and accreditation remains
- Allow for different time lines and approach due to demands of Ring of Steel, JCCR and Accommodation programme

Managed Desktop

The current desk top models in both the Police and Corporation is end of life and has failed to keep up with industry changes to support the end user experience. The Police environment is slightly more advanced based upon Windows 8 while the Corporation has a more urgent need for change. This necessitates two distinct programmes but ultimately utilising the same Technology Stack.

The Transformation Programme envisages;

- Replace life expired hardware for all users
- Implement a fully managed Desktop and mobile device model
- Implement Windows 10, Office 2016, Collaboration (Skype for Business)
- Implement a unified Technology Stack to enable the benefits
- Implement an appropriate VPN solution
- Single standard versions of 3rd party applications deployed to end users
- Implementation of a managed renewal cycle
- Reuse where ever possible the learnings, design documents and approaches developed in the Corporation as the first to market

But to implement a managed desktop as two separate programmes aligned to individual business requirements to;

- Deliver to low level business requirements

- Recognise different demands for mobile and smarter working
- Ensure security compliance remains in place
- Recognise the differences in demands for application compatibility

Collaboration Software

Collaboration software is the broker to enable organisation and cross organisation collaboration at the user and document level. Collaboration can give us the ability to federate services such as calendars and share documents.

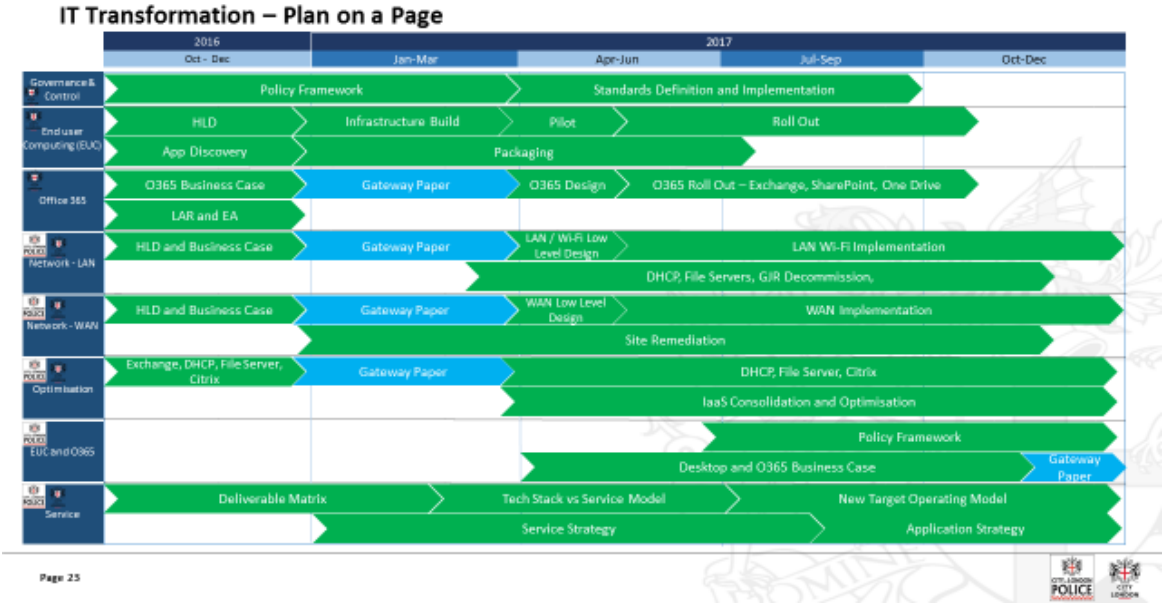
Office365 has been selected on the basis of value for money, return on investment, ability to select licenses appropriate to user's roles and alignment to the Technology Stack. The CoLP are in the process of validating the security model of the service offering.

The Transformation Programme envisages,

- Implementing collaboration software for mail, SharePoint and Skype for Business
- Deliver significantly lower IaaS storage and server costs
- Enhanced collaboration
- Separate tenancies for CoL and CoLP to ensure security boundaries are maintained
- Removing the need for future upgrades
- Mail box sizes up to 50GB per person
- Readiness for meeting the needs of current and future collaboration requirements

IT Transformation Road Map

The emerging Transformation Road map shows the Corporation on an earlier trajectory for the managed desktop and collaboration software with the Police requirements under development. The Network Transformation for the WAN and LAN are following the same glide path delivering the stated goals of a joint approach above. The Strategy for the Police is under development to align their requirements to Digital Policing.



This page is intentionally left blank

Appendix 2

City of London Police (CoLP)
IT Strategy
2020 Vision

Only to be read in conjunction with the Technical Design Principles Document)

Approved by IT Sub Committee 22.2.2017

Review 22.2.2018

Document Details

Version	Modifications	Author	Date
0.1	First draft	Rhys Lovegrove	27/01/2017
0.2	Internal review and amendments	Kevin Mulcahy	27/01/2017
0.3	Third draft following the request from the Police IT Strategy Board to reference in an appendix the CoLP Security Policy	Sean Green	02/10/2017

Approvals

This document requires the following approvals:

Name	Role	Signature	Date	Version
Peter Kane	Chamberlain		15/02/2017	0.2
Sean Green	Director of IT		15/02/2017	0.2
Alistair Sutherland	Assistant Commissioner		15/02/2017	0.2
IT Sub Committee	Endorse		22/02/2017	0.2
Finance Sub Committee	Endorse		02/05/2017	0.2
Police IT Strategy Board	Endorse subject to v0.03 changes		26/09/2017	0.2
Alistair Sutherland Police Senior Management Board	Endorse		11/10/2017	0.3
Police Committee	Agree			0.3

Distribution

This document has been distributed to:

Name	Role	Date of Issue	Version
IT Transformation Steering Group		January 2017	0.2
IT Steering Group		January 2017	0.2
Police Strategic IT Board		February 2017	0.2
IT Management team		February 2017	0.2
Police IT Strategy Board	Endorse	September 2017	0.2
Police Senior Management Board	Endorse	October 2017	0.3

Contents

1 Introduction and Context

The City of London Police (CoLP) are now at a point where it needs to re-evaluate both the demands it has for its IT services and how those IT services will be supplied. The current Technology stack has reached both the end of its supportable life and the end of user's tolerance for the current service offering.

This paper, which needs to be read in conjunction with the Road Map Design Principles, articulates the current problem definition, what we can learn from the past and how we can shape the future with a clearly defined strategy and road map. CoLP is a consumer of IT and ultimately its strategy is based on the services it needs to consume, market trends, The Local and National Policing Agenda's and the transformation required to enable those services. Strategy is about shaping the future and has 3 components:

- Diagnosis: analysing the environment or situation, i.e. making a diagnosis
- Guiding Policy: setting the Policy framework
- Action Plans: sequencing the tasks and activities

The key point is strategy is not a vision but is the defined action plan based upon the Policy Framework and the diagnosis of the current issues.

This document is concerned with the IT strategy and not the Information Management strategy which is a separate methodology linked to business strategy and business process.

IT is the enabling services and supporting infrastructure the business consumes, and as such is an enabler to the City of London 2017 Policing Plan. IT is critical to business success and for a modern Police Force it is essential that the underpinning IT and services are fit for purpose, and support the policing priorities of the force. The IT strategy should always support the overall force strategy, and so for CoLP it is vital that an IT service is delivered that supports the seven policing priorities of the force:

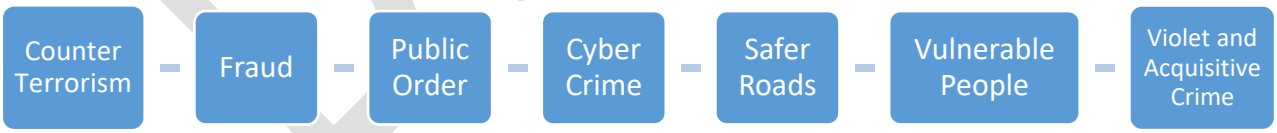


Figure 1 – Policing Priorities – City of London Policing Plan 2017

The CoLP IT Strategy will help to ensure that the force achieves its stated commitments across these priorities, in addition to ensuring appropriate technology is adopted in order to enable CoLP to on board key national change programmes across UK policing.

2 IT Core Principles

In order to ensure that an IT service is delivered that meets the current strategic needs of the force, whilst acknowledging the lessons learnt from previous IT services and infrastructure, the following key principles will be adopted around the IT Services for CoLP.

These principles will be applied throughout the adoption of new IT products and services, to ensure that they are suitable for supporting the needs to a modern police force. It is believed that the adherence to these principles will help to ensure that an effective and cost efficient IT service is provided, whilst ensuring that the maximum benefit is obtained from the product sets that are in place.

Stability: Services will only be adopted where they have been tested appropriately, are compatible with existing technical environments, are compliant with security policy and have a clear support and maintenance process.

Capability: The capability of systems and services to provide value for money, return on investment, business objectives and requirements will be assessed for every IT project and programme and in-services solution. Regularly review will take place to ensure capabilities are still being met throughout the lifecycle.

Adaptability: Wherever practical, IT services will be adaptive to change, and be able to flex and demonstrate continued service delivery, often as a result of external factors including legislative and regulatory change.

Resilience: All critical services will be demonstrably resilient through regular testing to provide the force with sufficient confidence to meet recovery time objectives.

Security Compliance: All services will be secure by design and subject to regular vulnerability and assurance processes. Regular review will take place to ensure that all IT services provided are compliant with national standards, to ensure continued connectivity to nationally provided services. (See Appendix 3 – CoLP IT Security Policy)

Commodity Based IT Services: All IT products and services will leverage the benefits available from Commercial off the Shelf (COTS) technology wherever possible. CoLP will “buy not build” where appropriate in order to provide an IT service based upon proven and reliable technologies. There will always be the need to assess specialist or bespoke IT products and services to meet the needs an operational police force, and so the COTS products will not be appropriate for all requirements.

Rationalisation: The capabilities and functionality from a set of core IT systems will be maximised wherever possible, enabling the force to operate a streamlined and efficient set of IT services to support operational policing.

Collaborative Working: The benefit of working with collaborative partners across the delivery of IT services will emphasised. Regular assessment of collaborative IT options will take place to ensure maximum efficiencies from working with blue light services, as well as other strategic partners.

Compliance with national standard: Alignment with both nationally led transformation programmes across the police service, as well as within central government initiatives to maximise contractual efficiencies across police IT functions, in line with Home Office guidelines.

Innovation: CoLP will seek to implement IT services that are both innovative and intuitive. Providing technology that enables the force to meet the challenges of both the modern crime prevention strategy, and the requirements of protecting a major city.

3 Industry Developments and Digital Transformation in Policing

The IT industry can be defined as a mature industry, with future developments now focused on lower costs and simplicity.

Further efficiency and productivity improvements in IT will come from leveraging new delivery mechanisms from cloud based service providers and aligning the service model to new ways of working.

The key developments are:

- The internet has become increasingly dominant in terms of how services are viewed and accessed
- The Cloud delivery models have reached maturity for use across UK Policing.
- Innovation is coming from how services are being delivered and consumed
- IT service models have transformed
- The Corporate IT function is de-skilling as the services move to the cloud
- Services are increasingly agile with a focus on mobility

These developments have come together to form the basis of Digital Transformation, which seeks to take advantage of these trends to deliver a better outcome for the enterprise. Digital Transformation can be defined as the end-to-end approach to modernising IT and is an effective approach to create and support a viable digital business. It has three key components following the strategic agenda;

- Defining the target state for their IT architectures
- Deciding which elements of the IT landscape (systems, people, and processes) need to change
- Determining the sequence and scope of change

The Police Service faces an unprecedented level of change over the coming period. The manner in which forces engage with the public will change dramatically, whilst there has been a widely publicised shift in crime types from traditional to modern digital and cyber crimes. The adoption of a number of major change portfolios across the UK Police Service will fundamentally change the way in which forces operate in the future. These include:

- The Digital Policing Portfolio,
- The Emergency Services Network
- The National Law Enforcement Data Service,
- Home Office Bio Metrics Service

These change portfolios will help forces to meet the demands of the Modern Crime Prevention Strategy, in addition to enabling forces to adopt changes in methods of public contact.
The IT Strategy for the City of London Police is to follow a Digital Transformation Strategy that addresses the failings and weaknesses of the past while ensuring the organisation is ready for these future challenges. This paper covers the road map for the underpinning services of the network, infrastructure, end user computing and collaboration services. More importantly it addresses how these services will be consumed, supported and the underlying policy frameworks. The major challenge for us in all this change will be how the IT department responds as we move away from building IT to consumers of IT.

4 The Diagnosis and business requirements

4.1 User Perception challenge

To change the IT department needs to be honest with itself on the current challenges and the perception gap between user expectations and the service and services being offered. More importantly we need to be honest with ourselves on the root causes and ensure we are a learning organisation that can work together to enable an enhanced IT offering. With the consumerisation of IT in many cases our users IT is better in a home environment than at work.

Current perception and reality of IT within CoLP can be summarised as;

- Reactive not Pro-active IT Service
- Underperforming systems
- Slow performance
- Outdated technology
- Poor Agile Working Capabilities
- Poor Service Management
- End user frustration
- Lack of credibility
- High levels of complexity
- Lack of understanding of a policing environment
- Lack of IT Visibility – Who, Where, How

No one root cause can link these issues but a number of themes have emerged;

- Lack of investment historically in IT
- Lack of architectural reference model
- Service and support landscape failing to keep pace with change
- Outdated and complex technology stack
- Built up technology debt
- Undocumented systems
- Poor understanding of the “as is” built environment
- Projects not fully transitioned into support
- Projects closed down before they had delivered their goals
- Overlapping technologies
- Sub optimal approach to out sourcing
- Not all IT services within the scope of the IT Dept

- Lack of clarity within the delivery model
- Transparency of Budgets vs. Service

To illustrate the point, we need to ask why does it take 3 days to deploy a new laptop when the industry standard is 45 minutes. Our last upgrade of the desk top environment moved us from Windows XP to Windows 7. This was forced on us by XP going end of life. The issue was that in the intervening 10 years the underlying architectural, support and delivery model had fundamentally changed. While the badge on the system says Windows 7 we are still managing the solution as though it was XP putting our technology 15 years behind in terms of improvements. The project exhibited all the attributes above and we can take some key lessons forward through our change;

- Upgrades are not about the technology but achieving improvements in business outcomes
- To achieve the outcomes, we must not only upgrade the technology but also the support and service model
- Methodology must be followed including being clear on acceptance criteria

4.2 Technology Stack Review

Following methodology, the starting point for the strategy has been an in-depth analysis of our technology stack in determining root cause of user frustration. The analysis helps us understand the as built environment, the components and impact of change and the sequence of events.

CoLP Technology stack - January 2017 (baseline)

USER										
Device Applications	Office 2010	Office 2007	Device Lock	McCain	Good	Visio 2007	Visio 2013	SCCM 2010		
	BitLocker	Business Apps	Project 2007	Project 2013	Met compliance	Office Enforcer				
Browsers & Viewers	IE 11	MS Silverlight	Jave (JRE)	Adobe Reader	Adobe Flash	IE 8	FX Logic			
Device Platform	Windows 7 Enterprise	Windows 8.1	Citrix	BlackBerry OS 5	Apple IOS					
Device Hardware	Viglen Desktop PCs	HP Laptops	Microsoft Surface	Lenovo Laptops	Analogue Conf Phone - Polycom	Lenova Docking Station	Blackberry	Door Access Controllers	Video Conferencing	DVD Writers
	Basic Nokia Mobile Phone	iPads	IP Cameras	Video Screens	iphones	Mitel Desk Phone	Panasonic Docking Stations	IP Conf Phone Polycom	Finger Printing	Monitors
	Airwave	Breatherlizers	Printers and Scanners	Barcode scanners	Doc Identity Checker	ANPR	Panasonic Tough Pads	Signature Pads	Mobile Printers	
SERVICE										
Applications	HR Origin	Exchange 2010	Business Objects	Forensics Case Mgt	iTrent	ESRI	Pronto	PNC	Holmes	Experian
	NSPIS Custody	NSPIS Case	Unifi	DIR	KIM Property	Sharepoint	PND	MetCad	Ident 1	PNLD
	Charter	Firearms	Centurion	KnowrFraud	VISOR	Custody CCTV	Voice Recording		Nabis	Acesco

Application Technology	MS Internet Information Server	Apache Web Server	Oracle JSP	Oracle Forms	Citrix XenApp	MS BizTalk 2010	Engress	APP V
	Oracle OBI	RDS						
Management Tools	Solarwinds	TSM Backup	IBM Endpoint Manager	Mutiny	VMware vCenter	Active Directory 2008	Group Policy	
	WSUS	Nessus	Good MDM	Sation	Blackberry Enterprise Server 5.x	SCCM	NetBackUp	
	SupportWorks	EPO	Lan Sweeper					
Security & Access	Cisco Firewalls	Bomgar	MS Certificate Services	JetNexus (Loadbalancer)	Site VPNs			
	Stonegate VPN	Gateways - multiple	NAC	SIEM	StoneGate Firewalls			
DATA								
Databases	SQL Server 2005 onwards	SQL Server 2005	SQL Server 2005 Express	SQL Server 2008	SQL Server 2008R2	SQL 2012	Oracle Database	MS Access
File Service	Windows File Service	Huddle	FTP Service					
INFRASTRUCTURE								
Server Platform	Windows Server 2003	Windows Server 2003 R2	Windows Server 2008	Windows Server 2008 R2	Windows Server 2012	Linux	SunSolaris	
Server Virtualisation	VMware	Hyper V						
Server Hardware	Hardware Servers	Agilisys IaaS						
Storage	HP DAS	IaaS Storage						
NETWORK								
Network/Telephony Devices	LAN Switching	WAN Routing	Wi-Fi Controllers & APs		Mitel VoIP			
	Mitel ACD	Switchers and Routers	Voicemail	ADSL Routers	Brent Phones			
Network/Telephony Links	O2 (Public Wifi)	BT Point-to-Point Links	Mobile Phone Network	BT Broadband (wires only)	ISDN30 Phone Service			
	Virgin Media MPLS	Dark Fibre						
Data Centre	GJR	New Street	Wood Street	Bishops Gate	Snow Hill	Power Gate	Welwyn	Tape Library Hammersmith

The components of our infrastructure are heat mapped and coded as follows

- Green – currently fit for purpose though may underperform due to other components
- Amber – needs attention, approaching end of life
- Red - either end of life, poorly architected, overlapping and ultimately requiring change

- Blue – Status currently being confirmed via exploratory activities

Coupled with this has been an in depth system analysis on the following components;

- Network and site surveys
- Exchange
- Fileservers
- Desktop
- Active directory
- Infrastructure
- Applications

The detailed analysis can be viewed separately but result in a number of themes to follow through in the CoLP solution design. In principal the critique of the technology stack and its components are;

- Poor understanding of financial model and real Total Cost of Ownership by IT and Change Programmes
- Lack of historical investment in IT Infrastructure
- No defined Policy framework
- Lack of understanding of the component interdependencies
- Little standardisation and optimisation
- Components implemented in silos
- Lack of investment in support and maintenance
- Poor transition and handover into support
- Components and the technology stack failing to meet business requirements
- Aging application stack, in particular national police systems

4.3 Risk Profile

Given the complexity and current state of the technology stack a number of emerging risks need to be highlighted and mitigated through the transformation. The lack of standardisation and architectural principles imposes unquantified security, business continuity and disaster recovery risks. A key component of the transformation will be to ensure we have effective and manageable risk profiles.

4.4 Design Principles and Business requirements

As we design the solutions we can now define a set of design principles and business requirements that all solutions must conform to;

Business Requirements

- Enhance the end user experience
- Deliver a platform to enable a more mobile workforce
- Enhance the reliability and functionality of our environment
- Align the user experience to modern ways of working
- Deliver collaboration to provide a connected workforce
- Place CoLP into best in class for Technology adoption and exploitation
- Provide our users with appropriate the tools to do their jobs
- Align user expectation and user perception

Design Principles

- Policy led design
- Remove complexity and simplify wherever possible
- Deliver end to end solutions
- Ensure the support model transforms in parallel with the technology
- Adaptable to current and future needs
- Alignment to industry trends
- The Technology Stack will be architected to best practice providing resilience and redundancy at all levels where cost effective and aligned to business requirements
- The Technology Stack will be designed to support CoLP requirements for cost effective ICT services
- Cloud solutions wherever possible
- Technology stack platform based around a single vendor where possible
- The technology stack will be maintained and software patched to the required levels
- The technology stack will be monitored and maintained at all times
- Compliant with PSN/P
- The technology stack will be fully documented at all times
- Aligned to good industry practice and architectural principles
- Eliminate vendor device proliferation and collapse functionality into minimum number of devices
- Acknowledgement/alignment with national IT roadmap led Police IT Company, The National Police Technology Council & National Change Programmes for Policing.

5 IT Strategy 2 Year Plan and Policy Framework

5.1 Phase 1 2017 – Strategy and Financial Planning

Strategic context

- Development of a strategic plan and financial model to deliver the required changes
- Corporation wide agreement on the strategic plan and financial model
- Agreement on Corporation Governance

Operational Deliverables

- Agreed Strategic Agenda
- Agreed Financial Plan
- Agreed Organisational Model
- Commercial and 3rd Party Contractual Framework

IT Core Focus

- ORGANISATION
    - Alignment to the strategy
    - Clear roles and responsibilities
    - Focus on transformation vs day to day
    - Removing gaps, and overlaps between internal and external IT service provision
- POLICY
    - Organisational policies mapped
    - Policies, reviewed, re-defined and linked to business requirements
    - Principles agreed with Key Stakeholders on both COL and CoLP

    - Defined metrics of change
- FINANCE
    - Confirm Corporate Governance
    - Map and define Finance Stakeholders in both COL and CoLP
    - Confirm alignment with Gateway Process
    - Define Financial Model

5.2 Phase II 2017 - Delivering the change

Strategic Context

- Delivering the agreed plan to time quality and cost
- Supporting the change agenda while keeping the business safe

Operational deliverables

- Network WAN and LAN Refresh & Implementation of Office 365
- CCCI and Applications Rationalisation
- IT Work streams to Support Accommodation Programme
- Commencement of deliverables for ESN
- Commencement of Digital Policing Programme
- Maintaining BAU while delivering the change
- Contract and commercial realignment

IT Core Focus

- ORGANISATION
    - Day to day delivery and customer focus
    - Operational delivery structures with management specialists and overlap with outsourcers removed
- PROCESS
    - Defined Standards linked to agreed Policies
    - Budget management
    - Corporate communications
    - Stake holder management
- BUSINESS AND IT
    - Business case management
    - Steering Groups
    - Business requirements
    - Maintaining visibility and the pace of change

5.3 Phase III 2018 – Shift from Build to Consume

Strategic Context

- Landing the change
- Benefit realisation
- Contract tendering

Operational deliverables

- 5-year plan for IT Services for CoLP
- Transition to EUDR for CoLP incl Windows 10

- Commencement of NLEDS and Home Office Bio Metrics
- Embedding the change
- Contract retendering
- New Target Operating Model (TOM) aligned to Operational context

IT Core Focus

- ORGANISATION
    - New Target Operating Model
    - Redefined service landscape and SLA's
    - New contractual landscape
    - Focus on service definition and delivery
- PROCESS
    - Procurement and tendering
    - Continuous service improvement
    - Demand management and optimisation
- OPERATIONAL MANAGEMENT
    - New structures and governance procedures
    - Commercial and contractual management
    - Financial controls and cost savings

5.4 Policy Framework

"A policy is a deliberate system of principles to guide decisions and achieve rational outcomes. A policy is a statement of intent, and is implemented as a procedure or protocol."

The policy set currently in use within CoLP was revised during the transition to the current managed service provider. Evidence provided from the current Key Performance Indicators and staff surveys, have identified areas where the IT Dept needs to improve. As part of the work to transition to the new IT operating model post the cessation of the current managed service contract, the policy set will be re-addressed to meet the requirements of the force. This will be carried out by IT in conjunction with the Strategic IT Board to ensure that the needs to the force are accurately represented.

Policy is key as they assist in the decision making process. They act as business requirements and ensure all changes comply with standard risk mitigation. Sub sections of these Policies will need endorsing by the business while others are for note and it will be IT's responsibility to ensure all change complies with the Policy.

A flavour of the policies includes;

- Finance and Investment Policy
- Security Policy
- Data retention Policy
- Environment management Policy
- Starters mover and leaver Policy
- Application Management Policy

6 IT Strategy and Components of Change

6.1 The components of change

The IT Strategy is to follow a Digital Transformation agenda, aligned to business requirements and addressing the underlying issues in systems, processes and people with a clearly defined Policy Framework.

Support Model and Service Landscape

- New Policy Framework
- Service strategy
- New support model aligned to the technology stack
- New Target Operating Model

These changes are to support the Refreshed Technology stack including;

- New Managed Desktop
- New Network
- Move to Productivity Services
- Unified Communications
- New Service Provision for Data Storage
- CCCI and Application Rationalisation
- Digital Policing Portfolio
- Mobile Technology and The Emergency Services Network
- National Change Programmes – NLEDS and Home Office Bio Metrics
- ERP – Back Office Services/Business Process Automation

This is supported by a programme of readiness and enabling works including

- Accommodation Strategy and closure of redundant data centres
- Application Delivery
- File server re-architecture
- Non-core sites remediation
- Consolidation and optimisation

6.2 Support Model and Service Landscape

The current IT service landscape is a break fix service based upon a legacy technology stack. As the technology stack transforms, the service landscape will need to evolve in tandem to a proactive, measurable environment to support consumption based IT.

The move to managed environments and cloud adoption requires different skills and metrics to support the change. As part of the strategy multiple services will move to the cloud supported by a new Service Management Framework based upon defined deliverables and metrics. New skills will be required in demand management; optimisation and consumption based pricing to ensure we deliver on our business case and reduce the Total Cost of Ownership of IT. This requires re-skilling the IT function as we move from technologists to service architects.

As the existing IT outsourcing service moves towards the end of its contract, services need to be re-tendered to new providers specialised in these services. Although a single IT service operates across both The Corporation of London (COL) and CoLP, due diligence will be carried out to ensure that any

services meet the specific requirements of a blue light service. This will be from the perspectives of use cases, security and compliance standards, and alignment with national policing IT strategies. This work will commence during 2017 in order to tie in with the cessation of the current IT managed service contract, and allow suitable time for the procurement of new services where necessary.

With increased remote management and automated support models the landscape and inevitably the Target Operating Model supported by new roles and responsibilities will also be refreshed. This process will ensure that any revised operating model for reflects the requirements of a 24/7 operational police force.

6.3 New Managed Desktop

Although the current desktop estate was replaced in 2015, and Mobile Data Tablets implemented in 2016, products will continually head towards end of life and must be updated. This will ensure CoLP keeps up with industry changes to support the end user experience, and ensure compliance with national security standards. This would incorporate:

- Implement a fully managed Desktop and Mobile Device Model
- Implement modern desktop operating systems and applications
- Implement a unified technology stack to enable the benefits
- Implement an appropriate VPN solution to enable reliable Agile Working
- Implementation of a managed renewal cycle
- Implementation of a future roadmap for all desktop software
- Rationalisation of additional propriety third party products

In this context, a fully Managed Desktop has the following attributes;

- Standard OS build for all users aligned to CoLP ICT and Security policies
- Standardised patching and management for all end user devices
- Applications managed and deployed centrally
- No local software installs
- Active Directory designed and maintained to best practice
- Policy driven environment
- Zero touch support and smart access to applications

The migration to a new managed desktop will provide the reliable technology to enable staff to work both an agile and a mobile manner. This will provide significant benefit to the force priorities around Counter Terrorism, Public Order, Safer Roads, Vulnerable People and Violent & Acquisitive Crime.

6.4 Network

A new network following "the expect to connect" goal. The current network comprising of the local and wide area network is end of life and cannot support future collaboration objectives. Consistent and repeatable failures are diminishing CoLP's ability to operate. Bandwidth constraints at multiple sites are failing to keep up with user demands, and will not provide the capabilities for major digital transformation projects such as The Ring of Steel, Digital Investigation & Investigation, and The Joint Command and Control Room (JCCR).

The plan envisages;

- To deliver an upgraded network for CoLP – both LAN and WAN
- To enhance the end user experience and expect to connect

- To improve resilience and redundancy
- To ensure security policies are adhered to and accreditations remain
- Ensure the solution is supportable and maintainable
- To facilitate bandwidth for the provision of digital first technologies
- To upgrade all End Of Life equipment
- Support agile working practices with a corporate WiFi solution
- To enable future collaboration, both with COL and other partners
- To implement a new support model
- Transition all network attached equipment on to the new network
- To decommission the old network
- Transition into support with new tools, training and support agreements

The implementation of new networking will provide CoLP with reliable and scalable technology. This will ensure that staff can access services in an efficient manner, minimising disruption caused by slow running and network outages. This will also provide the infrastructure to support major change programmes such as The Ring of Steel, The Accommodation Programme and The Digital Policing Portfolio, thus providing significant benefit across all of the forces key priorities

6.5 Productivity Services

The current Microsoft Office suite, SharePoint, and Exchange infrastructure within CoLP are rapidly heading towards end of life. With an upgrade pending, the optimal Total Cost of Ownership (TCO) model suggests moving Exchange and SharePoint to commercially based cloud services . This gives us multiple benefits including:

- Optimal Total Cost of Ownership (TCO)
- Reduced incidents
- Enhanced performance
- Significantly lower IaaS costs
- Removing the need for future upgrades
- Lower storage costs and enhanced collaboration with One Drive
- Mail box sizes up to 50GB per person
- Ability rationalise additional propriety third part products

The adoption of this technology will ensure that CoLP are in a position of readiness to meet the forthcoming requirements of the national Digital Policing Portfolio. This will also provide the underpinning technology to support all seven of the forces key priorities.

6.6 New Service Provision for Data Storage

As part of the programme to transition to the existing IT Managed Service, the vast majority of the IT server and storage infrastructure has been moved to the externally hosted IaaS Model (Infrastructure As A Service). The exception to this being data hosted at IL4 and above (in legacy information classification standards).

As part of the work to transition from the current managed service structure, work will be carried out to align to commercially available cloud based storage technologies. This will provide the scalability and capabilities to support the transition to the digital policing portfolio, in addition to the delivery of efficiencies against the existing storage models. CoLP would seek to adopt this approach for data at all security levels, leveraging the most appropriate supplier/suppliers to achieve this.

CoLP will seek to align with any strategies or commercial ventures managed by The National Police IT Company, in order to leverage benefits across the UK police service.

The optimal model suggests moving to an appropriate cloud based solution using an appropriate vendor. This provides multiple benefits including:

- Optimal Total Cost of Ownership (TCO)
- Adoption of consumer based approach to secure data storage
- Enhanced performance
- Decoupling of IT infrastructure from the physical estate
- Reduced physical space requirement for server rooms
- Improved Disaster Recovery and Business Continuity
- Ease of meeting increased data storage requirements for Digital Transformation
- Improved support capabilities, reducing reliance on “in house” staff

The transition to such a storage strategy will provide scalable and reliable infrastructure capable of supporting increased data storage requirements around areas such as Counter Terrorism, Fraud Prevention and Cyber Crime. Additionally, adoption of this model will ensure the disaggregation of IT storage from the physical force estate, supporting the forces Accommodation Strategy.

6.7 Unified Communications

This represents the next level in user experience and collaboration by moving our telephony service to the cloud. Work is underway to explore our options for the completion of Internet Protocol Telephony within the force, and as part of this, the benefits of the transition to a Unified Communications platform will be assessed.

The adoption of this technology will provide the technology to enable police officers to communicate and share information easily and effectively with partner forces, and other agencies including the COL. The functionality that is available would provide significant tangible benefits for the force when managing major incidents, and would therefore support the priorities of the force in particular around Public Order and Counter Terrorism.

The benefits of this would include:

- Optimal Total Cost of Ownership (TCO)
- Enhanced Communication Methods including Instant Messenger and Video Conferencing
- Leveraging commercial cloud based products to enable communication with other partners
- Improved briefing capabilities to operational police officers
- Enhanced Communication Capabilities for Gold and Silver Command

6.8 CCCI (Crime, Case, Custody and Intelligence) and Application Rationalisation

A number of key operational policing applications used by CoLP are rapidly heading towards end of life. They are based upon old technologies, and do not provide the capabilities required to meet the goals of the digital Investigation & Intelligence Vision, and the Digital First Vision. This provides the force with a unique opportunity to implement a single system capable of managing multiple policing functions. The force will collaborate with the East Mids region for the provision of a single system across 6 forces.
The benefits of this include:

- Optimal Total Cost of Ownership (TCO)
- Enhanced Crime and Intelligence Capabilities,
- Rationalisation of multiple legacy systems into one database, enhancing the identification of the golden nominal
- Enhanced reporting capabilities
- Ability to meet the requirements of the Digital Case File and Digital Public Contact
- Functionality to deliver Track My Crime and Online Crime Reporting
- Cross Boarder Data sharing with the East Mids Region (Lincs, Notts, Derbys, Leics and Northants).
- Reduction in TCO for future functional requirements
- Modern technology to ease alignment with existing mobile data platforms other applications
- Consumer based storage model, providing capabilities to store increased volumes of digital data.

CoLP will maximise the benefits of this application by ensuring this will be the panacea for operational policing functions, with additional systems only purchased if functionality cannot be provided within CCCI.

The adoption of the CCCI Project will provide the force with modern technology to manage multiple areas of the policing model from a single source, thus supporting a number of the forces key priorities including Counter Terrorism, Public Order, Safer Roads, Vulnerable People, and Violent and Acquisitive Crime. This will provide the efficiency and effectiveness to meet the concerns raised of CoLP within The Peel Report.

6.9 Digital Policing

There is a significant shift in policing to adopt the technologies that are required to support the national digital policing agenda.

“By 2020, Policing will have efficient, effective, consistent, accessible and secure capabilities for digital public contact and the capture, exploitation, storage and sharing of digital intelligence and evidence.”

In recognition of this three national programmes have been initiated to support the development of digital policing capabilities under the auspices of the Digital Policing Portfolio

• **Digital Public Contact -** the approach to enabling public engagement with policing in the digital age (Chief Constable Simon Cole)

• **Digital Intelligence and Investigation -** the capabilities required to respond to online crime, develop intelligence and investigate the digital footprint (Chief Constable Stephen Kavanagh)

• **Digital First** – how evidence can be stored and shared with partners and the CJS (Chief Constable Giles York)

We will work closely with key stakeholders across the force to understand the impact of the digital policing agenda on operational processes, and develop technical roadmaps to support this. We will seek to implement commercial cloud based technologies wherever appropriate to support this portfolio of work, leveraging the benefits of proven productivity services and software. We will seek

to adopt commercial cloud storage and communication platforms as part of this transition, to readily provide the capabilities and capacity necessary to the digitisation of services.

CoLP are an active member of The National Police Technology Council (NPTC), and have played a part in the commissioning the three national enabling bids. Those being:

- Security Operations Centre (SOC)
- Identity and Access Management (IAM)
- Productivity Services.

As defined by the Director of the NPTC, these bids will enable:

"All UK police forces will have a secure platform and national standards that enable new ways of working and collaborating; while maintaining the local decision making of the autonomy of individual forces to maintain control their of digital assets"

CoLP will actively participate as a pilot force for the discovery phase of these bids, ensuring that the force aligns with the national vision for police IT, and leverage the benefits from this national approach, both commercially and in terms of functionality. The adoption of technology to support the Digital Policing Portfolio will enable us to provide solutions capable of supporting a number of the forces key priorities, including Fraud, Cyber Crime and Counter Terrorism, in addition to aligning the way the force engages with the other key elements of the legal system.

6.10 Mobile Devices and Emergency Services Network

The emergency services mobile communications programme (ESMCP) will provide the next generation communication system for emergency services and other public safety users. This system will be called the emergency services network (ESN). ESN will be a mobile communications network with extensive coverage, high resilience, appropriate security and public safety functionality.

A portfolio of mobile devices will be supplied that will provide capabilities to replace existing airwave radio equipment, in addition to enabling many of the capabilities that are provided by forces own mobile data solutions. Since 2014, CoLP has carried out work to implement a portfolio of mobile devices to support the agile and mobile working requirements of the force. This includes the prioritisation of laptops for staff, and the delivery of ruggedized tablet devices to front line officers.

We will ensure that the future portfolio of devices used by CoLP, and the underpinning technologies, align with national strategy and technology stack for ESN. We will work with key stakeholders in the force to identify a CoLP mobile device catalogue that meets the needs of officers and staff, whilst maximising the benefits of the ESN technology stack. We will not implement technical solutions that are in direct contradiction of the ESN technology stack. The provision of ESN devices with integrated critical voice and broadband data services will enable rationalization of the existing mobile device estate, enabling the force to address financial pressure in this area.

The implementation of such technology will support the forces key priorities around Counter Terrorism, Public Order, Vulnerable People and Violent and Acquisitive Crime, by providing and efficient and effective mobile communications platform across emergency services and its partners.

6.11 National Change Programmes

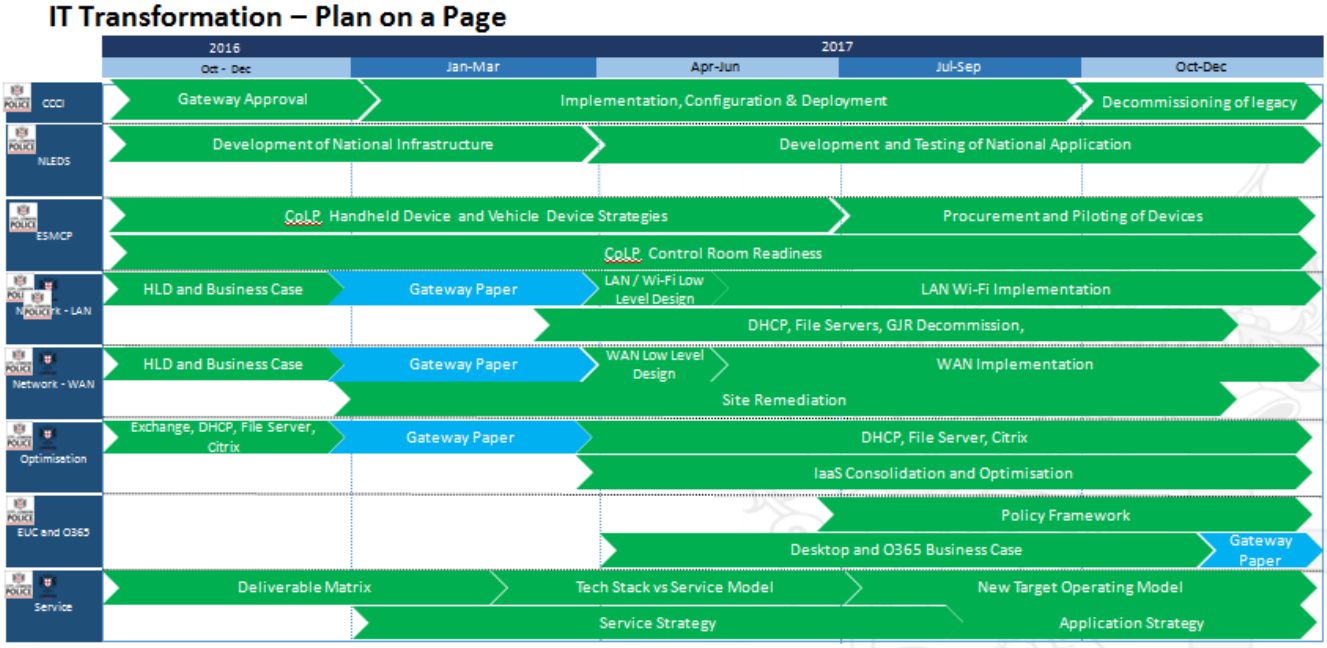
We will seek to align the applications and infrastructure roads maps that we deliver, with the requirements of national change programmes across policing. We will provide the appropriate levels of horizon scanning to ensure that there is a detailed understanding of what programmes such as The Home Office Bio Metrics Programme and The National Law Enforcement Data Service (NLEDS) will deliver. This will ensure that the force does not duplicate any of this new functionality in its current or future applications stack, and we will ensure that any infrastructure solutions implemented take into account the migration of UK policing to these new national initiatives, acknowledging the shift to centrally hosted services, will enable forces to share data in more intelligent manners, providing the technology required to support the priorities of both UK policing as a whole and CoLP.

6.12 Readiness and enabling works

This is a series of projects required as readiness criteria to support the broader delivery and fix a number of underlying performance issues in the environments. These projects include;

- **Accommodation Strategy and closure of redundant data centres** – the separation of IT infrastructure from the physical estate, and the subsequent rationalisation of data centres underpins the Accommodation Strategy. We are working to implement solutions that enable the move of staff across the estate, in remediation of IT infrastructure to allow the closure of buildings.
- **Application Delivery –** applications are currently installed directly onto devices. This causes significant issues for the force due to underlying software products, testing and related remediation. The ability to deliver applications in a virtual manner is an urgent requirement to enable continued use of the existing applications stack.
- **File server re-architecture** – the current solution is one of the critical components leading to poor end user performance. The analysis indicates a need to restructure the data, apply policy and re-architect to provide a fit for purpose business solution that meets end user performance requirements
- **Non-core sites remediation** - prior to the network refresh there is a requirement to perform remediation works across the estate to bring the environments up to standard to prepare for the new network. This includes removing substandard cabling, cleaning up comms rooms and providing standard racking for the new network equipment.
- **Consolidation and optimisation** – the move to IaaS was a lift and shift leading to high costs being incurred to host our infrastructure. This programme is focused on consolidation and optimisation to significantly reduce our IaaS costs and remove unwanted components. Standard cloud adoption methodology is to transform and then migrate to reduce the impact of consumption based pricing which was by passed in this case.

7 IT Strategy and Strategy Road Map



The Strategy Road Map has been designed to

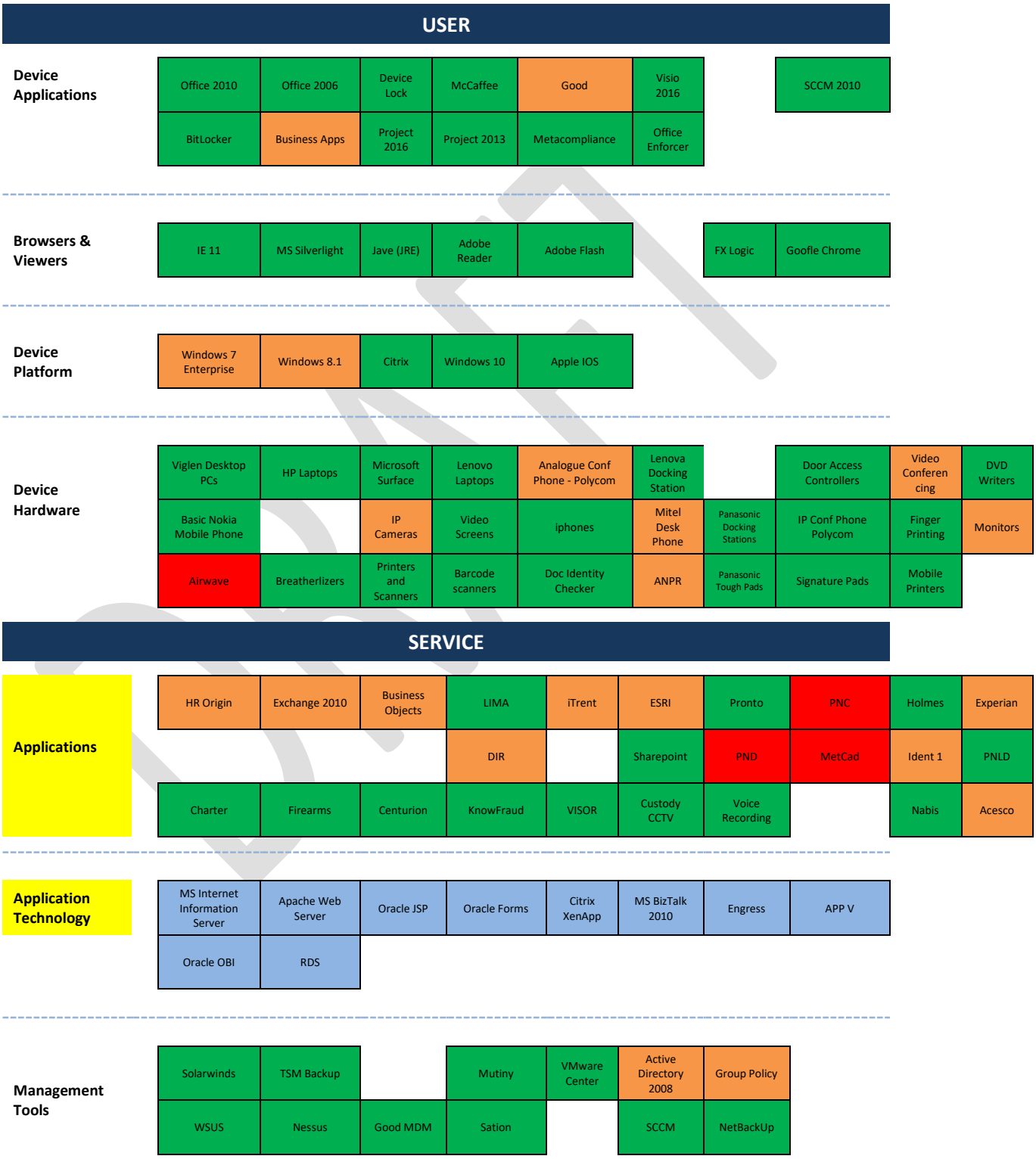
- Minimise business impact
- Reduce the impact of rework and change
- Sequence the changes to deliver maximum user benefit
- Follow good industry practice
- Understand the interdependencies with other programmes such as ring of Steele and Accommodation Programme
- Be clear on readiness criteria and enabling works
- Ensure we are addressing risk

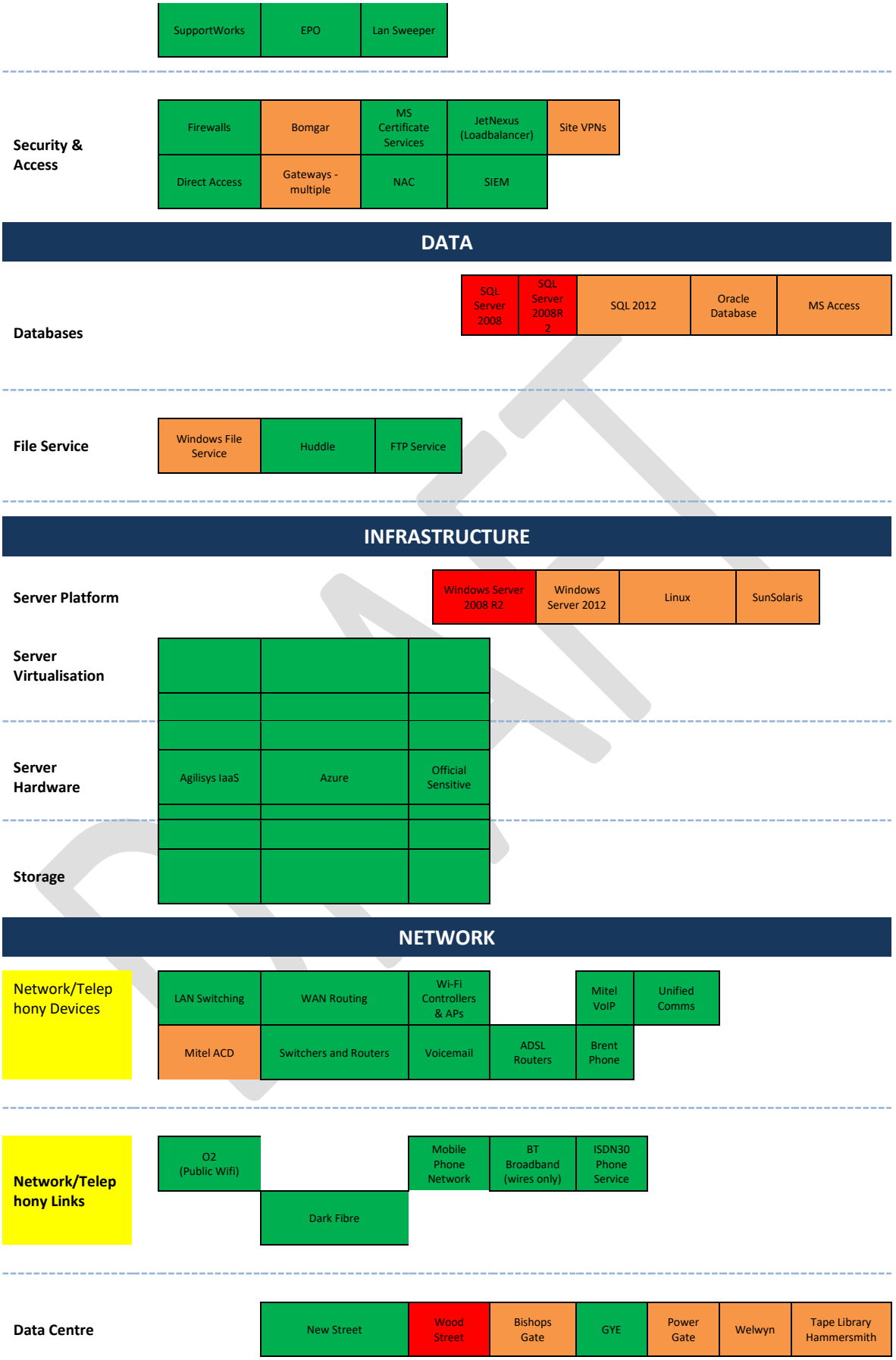
Sequencing the events is key to minimising the Transition costs and delivering the optimal business solution.

8 IT Strategy and the future Technology Stack

The IT Strategy will deliver the following simplified Technology Stack post Transformation with further works on applications and mobile solutions.

CoLP Technology stack - December 2017 (baseline)




SupportWorks
EPO
Lan Sweeper
Security & Access
Firewalls
Bomgar
MS Certificate Services
JetNexus (Loadbalancer)
Site VPNs
Direct Access
Gateways - multiple
NAC
SIEM
DATA
Databases
SQL Server 2008
SQL Server 2008R 2
SQL 2012
Oracle Database
MS Access
File Service
Windows File Service
Huddle
FTP Service
INFRASTRUCTURE
Server Platform
Windows Server 2008 R2
Windows Server 2012
Linux
SunSolaris
Server Virtualisation
Server Hardware
Agilisys IaaS
Azure
Official Sensitive
Storage
NETWORK
Network/Telephony Devices
LAN Switching
WAN Routing
Wi-Fi Controllers & APs
Mitel VoIP
Unified Comms
Mitel ACD
Switchers and Routers
Voicemail
ADSL Routers
Brent Phone
Network/Telephony Links
O2 (Public Wifi)
Mobile Phone Network
BT Broadband (wires only)
ISDN30 Phone Service
Dark Fibre
Data Centre
New Street
Wood Street
Bishops Gate
GYE
Power Gate
Welwyn
Tape Library Hammersmith

Glossary of terms and Abbreviation

Glossary of Terms	
ESN	Emergency Services Network
ESMCP	Emergency Services Mobile Control Platform
NLEDS	National Law Enforcement Data Service
SLA	Service Level Agreement
KPI	Key Performance Agreement
TCO	Total Cost of Ownership
COL	Corporation of London
CoLP	City of London Police
ICT	Information and Communcations Technology
WAN	Wide Area Network
LAN	Local Area Network
IAAS	Infrastructure As A Service
CCCI	Crime, Case, Custody and Intelligence
CJS	Criminal Justice Service
NPTC	National Police Technology Council
JCCR	Joint Command and Control Room
TOM	Target Operating Model

Appendix A – CoLP IT Security Policy (see attached document)

This page is intentionally left blank

Force Information Security Procedures Manual

Not Protectively Marked

Reference Information

Responsibilities	
Name of Policy that this SOP is attached to:	Force Information Security Policy
Name of SOP author/reviewer	Director of Information
Unit or Department:	Information Management Services
Directorate owning this SOP:	Intelligence & Information
Version control	
Date of latest version:	30 August 2014
Date Published:	*Strategic Development only*

Contents

A Procedures Manual Conext

A.1 Preface

Information security is vital to the Police Service to aid the quality, availability and management of its valuable information resources.

Security is a process, not a product; it is a management policy, strategy and tactic, fundamental to the well-being of every organisation in the modern digital world. Information security is a foundation for quality management processes, including Service Management (e.g. ITIL and ISO/IEC20000); of determining what you want to do and why, within applicable constraints (business, operational, statutory and governmental); doing it safely and securely and checking it is being done to the required standards. Security management is also an important component of change management and the continuous service improvement process.

Good security is not a goal, a target, a business model in its own right. It is a business enabler; a tool to facilitate safe and legitimate transactions for the business. Lack of appropriate security planning and management controls can lead to serious threats to the business.

All managers and users must play their part in delivering the 5 essentials of Information Security (Infosec):

1. **Confidentiality** – assuring information is available only to those authorised
2. **Integrity** – assuring information is not altered accidentally or deliberately
3. **Availability** – assuring information is available when it is required
4. **Non-Repudiation** – assuring inability to deny actions carried out
5. **Audit** – assuring records of who did what and when are maintained

Absolute security is impossible to attain, and ill-considered delivery will be ineffective and can be a financial and operational barrier to business

efficiencies. Risks must be weighed against the business advantages, and appropriate risk management decisions made to efficiently and lawfully deliver the required service at as low a risk and cost as can be achieved. This is usually achieved by the Project Manager, Business Process Owner (or SRO), Accreditor and SIRO working together to assess the business requirements, risks and countermeasures, via the Risk Management and Accreditation Document Set (RMADS) process, and support of the security and operational requirements by adequate technologies, training and documentation for all users. This delivers operational efficiency whilst assuring compliance with national and Force Information Security Policy.

The City of London Police (CoLP) works within the national frameworks of ISO 27001, HMG SPF, the Police Community Security Policy (CSP), the Community Code of Connection (CoCo), and the Code of Practice for the Management of Police Information (MoPI) locally encapsulated into the Force Information Security Policy (FISP).

Police IT networks and systems are part of the National Critical Infrastructure, requiring a wider viewpoint than just City of London Police and national policing. This precludes any overseas access or processing without robust controls which may be demanded by the RMADS review or Data Protection Act. The City of London Police follow the HMG Security Policy Framework should used as context for requirements within the UK/HMG national information security scheme.

A.2 Audience

This procedures document is suitable for, and should be made available to, all staff and users of City of London Police IT systems and information. Non-employee users (such as Local Authority partner staff, contractors, 3rd party suppliers or temporary agency workers) should be given a copy of the FISP and this procedures manual by their CoLP sponsoring manager and briefed with their compliance responsibilities prior to allowing access. The document may be published to non-users, the public and any requesting parties. The document is structured to facilitate review of single sections most appropriate

to the reader. Most users will obtain good practical guidance from Section F Personal Compliance; Managers should read the whole document and departmental users should, at a minimum, read the appropriate sections.

A.3 Understanding Risk

The Police Service is adept at risk management in relation to violence and other physical criminality. With the increasing demands for widespread use of IT, high security and sharing outside of the Police, information assurance must become a standard part of IT and governance in day-to-day processes and operations.

All information storage and processing – whether paper based or electronic – has weaknesses (or 'vulnerabilities'), which may be exploited by human frailty or inappropriate use, through to organised 'hacking' into Police systems to access information. To appreciate the risk, and hence what can be done in mitigation, two basic factors need to be considered:

(i) the likelihood of it happening

(ii) the impact if/when it does.

Virus threats provide a simple example:

> The likelihood is very high (there are hundreds of thousands of viruses in circulation and most home and SME personal computers have inadequate protection against them)
> The impact on the Police network can be very high – it may shut down the local Force network, including emergency calls, and cause wholesale disconnection from PNC and other vital Police systems, ultimately risking staff and public safety.

Deploying an effective, organisation-wide anti-virus (AV) system can reduce the risk to an acceptable level. But a single PC deployed without AV can immediately raise the likelihood and impact back to 'very high' by (accidentally

or otherwise) plugging into the CoLP network or by using a removable storage device, then connecting that to a network PC. Repeating the same behaviour can cause risks to other sites (for example, a school, Local Authority, Partner's site).

Another risk example is sharing sensitive information by email across the open Internet, where there is a high probability of unauthorised access. This may put vulnerable persons at risk, cause loss of public confidence and render CoLP liable for compensation and/or prosecution – an unacceptable level of impact, and a breach of Police integrity.

Without appropriate training & understanding it is likely staff will not act in line with statutory obligations under the Data Protection Act and MoPI, to the detriment of the public and staff. The personal impact on the affected people can be profound; the professional impact on CoLP can also be high.

Over 70% of information security incidents are caused internally, by authorised users. Most of these are not due to malicious/unlawful intent, but by well-meaning people striving to do their job well, who do not understand risk management and have not been appropriately trained in information security awareness. Lack of IT and information security training raises the impact likelihood to unacceptable levels and facilitates poor business practice.

Provision of 'sensitive' information on the CoLP Intranet, will mean it is made available to all computer account holders, employees – unless specifically hidden behind access control mechanisms.

Where 'sensitive' or 'personal' information is involved, the Force does not want to publish to people without a real 'need to know'? Users must therefore always consider:

(a) who needs to know and why?

(b) assure appropriate availability separation – how are they going to keep it secure?

Technology can reduce the likelihood of security events, subject to staff not by-passing the technical and procedural controls, but cannot reduce the impact should an incident occur. It is thus important everyone is aware of information security risks, has good training, and complies with CoLP and national information security policies.

B Strategic Perspective

Information and Communication Technology (IT) must be deployed, with information strategies, to support the process of providing effective and efficient Policing services. These systems must be developed, operated and maintained in a safe and secure manner.

The aim is to provide information facilities for users. There are management and legal issues which need to be considered to ensure the effective and appropriate use of information technology.

Information is an asset that, like other important business assets, has value to City of London Police and consequently needs to be suitably protected. Information security protects data and its owners and subjects from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments and Policing efficiencies.

Strategic Aim:

“To ensure that all Force information is kept secure and only accessible to those who are authorised to have access to it, and to be available when they need it”

City of London Police will allow the use, access and disclosure of information assets only in accordance with stipulated procedures and in conformance with applicable laws, regulations and directives.

It is City of London Police policy to ensure:

1. The Confidentiality of all Force information, whether electronic or paper-based
2. The Integrity of the information by ensuring its accuracy and completeness
3. The Availability of information systems and the information therein whenever required
4. That Information is disclosed only to those authorised to receive it

5. That Information so disclosed is used only for authorised purposes
6. That Regulatory and legislative requirements are met
7. That no IT systems handling protectively marked or personal information are to be made live prior to formal accreditation
8. That all staff and users will be made aware of their obligations with regard to Information Security
9. That each computer system/information process has an accredited set of Security & Data Protection Operating Rules where required by accreditation.
10. That Protection will be through an appropriate combination of personnel, physical, procedural, technical and management security controls.
11. That Enhanced security protection will be provided for information assets that are identified as being key to Force operations or are highly-valued under GPMS or GSC[1]
12. The Information Standards & Policy Group (ISPG) shall be responsible for all policies with respect to information gathered, stored and processed as part of any information system, whether manual or computerised
13. The Information Security Manager will have direct responsibility for maintaining the policy and providing guidance on its implementation
14. Divisional Commanders and Heads of Departments will be responsible for implementing the policy within their areas, and for monitoring adherence by their staff
15. All users are aware that it is their responsibility to adhere to this policy.

1 GCP comes into effect on 2nd April 2014, replacing GPMS

B.1 Importance of Information Security

City of London Police has a significant investment in computer systems and communications networks. City of London Police is dependent upon criminal justice and other personal information, acquired from numerous sources, which is stored and processed on its computers and the management information that is generated from the data. Increasingly other criminal justice information is remotely accessed using CoLP networks (for example PNC, PND). Failure to maintain appropriate levels of information security could incur significant costs and adversely affect the Force in numerous ways:

1. Loss of information and/or computer processing facilities
2. Loss or unauthorised disclosure of sensitive information relating to individuals and/or other Police information being made available to interested parties (which may include organised crime)
3. Loss of public credibility and confidence, especially via bad publicity
4. Business activities being fully or partially suspended, including prosecutions
5. Loss of accreditation to use other Criminal Justice and external systems
6. Unlawful/criminal manipulation of information, money or goods
7. Having to restore the data, computer programmes and/or equipment
8. Threat to Police or Public safety
9. Payment of compensation and/or civil/criminal fines
10. Prosecution or internal disciplinary action against City of London Police users.

It is therefore essential that there is preservation of the confidentiality, integrity and availability of information held not only electronically within internal systems but also on paper, microfiche, floppy discs, USB drives, portable computers, portable hard disks or CDROM/DVD.

B.2 Objectives

The objectives of this Force Information Security Procedure are to protect City of London Police's information through clear direction and guidance to ensuring that:

1. Clear guidance is provided to all users
2. All users of City of London Police systems, other Criminal Justice entities and the public are confident of the security, accuracy and integrity of the information produced and used
3. Operational damage and interruption caused by security incidents are minimised
4. Confidentiality of personal and other sensitive information is assured
5. All legislative and regulatory requirements, as well as Police mandated standards, are met
6. City of London Police Information Technology is used responsibly, securely and with integrity at all times.

B.3 Scope

This procedure applies to all users granted access to City of London Police's information (paper or electronic), communications or computer facilities and their associated networks. Unless a specific formal exception is granted, all elements of this procedure shall be treated as mandatory within City of London Police.

'Users' include all employees, temporary employees, contractors, agency staff, as well as external partners, suppliers and support people who may be granted access to City of London Police systems and/or information.

B.4 Principles

The principles of Information Security applied by City of London Police are based on the HMG Security Policy Framework (SPF), ISO/IEC27001 and the (Police) Community Security Policy (CSP) and include:

- Physical and environmental security.
- Risk assessment and business impact analysis.
- Access control.
- Asset management.
- Human resources security.
- Communications and operations management.
- Information systems acquisition, development and maintenance.
- Compliance.
- Information security incident management.
- Business continuity management.

B.5 Statutory Compliance

Some aspects of the City of London Police's security will be governed by statutory legislation. Data protection and privacy must be ensured as required in relevant legislation, regulations, and Police standards, and where applicable, contractual clauses. Key information records must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and Police requirements.

The City of London Police fully supports lawful obligations on the Police, and many ACPO guidance documents are available within the service. Relevant ones should be consulted in addition to this procedure.

All infosec areas are also governed by National and Police standards, including:

1. HMG Security Policy Framework (SPF)

2. National (Police) Community Security Policy (CSP)
3. Code of Practice on the Management of Police Information (MoPI)

B.6 Implementation and Governance

The Force Information Standards and Policy Group (ISPG), chaired by an ACPO member (normally the SIRO), are responsible for establishing the required information security policies and standards and ensuring compliant delivery. The ISPG will periodically review the Force Information Security Policy to assure ongoing compliance and business relevance.

A subset of the ISPG, chaired by an ACPO member, forms the governance body for City of London Police implementation of PKI and similar services. This is known as the PKI Management Authority (PMA).

Internal and external audit will periodically evaluate security controls while undertaking audit reviews in addition to undertaking specific Information Security audits on a regular basis.

All potential breaches of Information Security, suspected or actual shall be reported and investigated by appropriate bodies (determined by the breach) with serious breaches nationally notified to NPIRMT/PolWARP.

Information Risk will be assessed in accordance with the Information Systems Risk Management procedure and managed in accordance with the Force Risk Management Policy.

B.6.1 Individual Responsibilities

The Accounting Officer (AO) is responsible for lawful and effective business use of Police information within City of London Police. This role is held by the Commissioner of the City of London Police.

The Force Senior Information Risk Officer (SIRO) is responsible for ensuring appropriate risk management and controls are emplaced within the Force.

This role is be held by the Assistant Commissioner of the City of London Police.

The Departmental Security Officer (DSO) is responsible for all aspects of Protective Security which includes physical, personnel and information security as defined within the Security Policy Framework.

The Chief Force Information Security Manager is responsible for ensuring appropriate information assurance controls and risk management is in place for all systems and acts on behalf of the SIRO to accredit their use. In addition the CISO ensures compliance with relevant legislation, including MoPI across the organisation. This role is held by the Director of Information.

The Force Information Security Manager (ISM), more commonly known as 'ISO' within the Police Service, is responsible for policy, assuring compliance, ensuring audits are conducted, together with and local and national incidents and compliance reporting.

The Head of IT is responsible for ensuring the IT Services department operates in accordance with statutory, regulatory, contractual, and business requirements.

The Information Access Manager is responsible for day to day assurance of Data Protection and Freedom of Information and compliance.

The IT Security Officer is responsible for ensuring security technologies and procedures are emplaced and guiding IT Services to lawful and policy-compliant delivery of IT services.

The IT Network Manager is responsible for ensuring that the networks and communications, operating systems and support software and computer centres are secure and meet Policy requirements. IT is responsible for implementation of the IT specialist technical controls.

Information Asset Owners shall value the information they are responsible for and work with project managers, IT Services and users to assure appropriate controls are emplaced and enforced.

Local managers must undertake regular assessments of security risks within their own areas to ensure that the implementation of controls complies with MoPI and the local security procedures (this document) and for ensuring security training is provided to all staff and users within their managerial control.

All staff must accept responsibility for initiating, implementing and maintaining security standards within the force, ensuring they are operationally aware of MoPI.

All users must accept responsibility for maintaining standards by conforming to those controls, which are applicable to them. In particular users must be aware of the risks of introducing unapproved equipment or software onto the network, inappropriate use of the Internet, of sending sensitive information via public (ie Internet-based) email and of inappropriate (or unlawful) use or sharing of Police information externally.

B.6.2 Official Secrets Act

All staff shall be aware/made aware that they are bound by the provisions of the Official Secrets Act 1989, which offers protection under criminal law to official information in certain specialised categories.

The Official Secrets Act 1989 makes it an offence to disclose official information which could be detrimental to the national interest. This definition includes disclosing information without lawful authority which results in the commission of an offence, aiding an escape from legal custody, or impedes the prevention or detection of crime.

Under the new GSC[2] there is an even greater emphasis placed upon personal responsibility for making decisions around the sharing and release of information.

C Acceptable Use

This procedure should be read in conjunction with the Force Acceptable Use Policy, which users must accept before accessing Force systems.

The basic acceptable use tenet is that all City of London Police IT systems and information are only authorised for legitimate business use; private use is normally disallowed. The acceptable use policy is separately documented in detail.

D Exceptions Management

D.1 Objective

To provide a process to enable exceptions to the Force Information Security Policy and Procedures Manual to be recorded, reviewed, authorised/rejected, and audited; and manage any appropriate appeals.

D.2 Justification

As the requirements of the Force become more complex, particularly with the growth and development of national, local and criminal justice partnerships, occasionally there is a strain on compliance with FISP, CSP, MoPI, (CJX) Community CoCo and ISO/IEC27001 security policies and standards.

Unmanaged non-compliance (or non-conformance in quality management terms) causes risk-conflict, audit difficulties and potentially affects security accreditation in addition to infosec problems. But, for valid business reasons, it may be occasionally necessary to provide and subsequently manage a concession, which technically falls outside of the current security policies, but where the risks can be considered manageable and justified.

2 GSC, the new Government Security Classification, comes into general use on 2nd April 2014 across government.

D.3 Operation

Applications for an exception/concession must be made by the owning manager and approved prior to implementation. Applications must be in writing and sent to the Chief Information Security Officer (the Director of Information).

E Compliance

E.1 Legislation

All relevant statutory, regulatory and contractual requirements shall be complied with. The key laws associated with Police Information and their uses are included in the following table.

Act	Main issues addressed
Freedom of Information Act 2002	Public access to Police and Criminal Justice information
Human Rights Act 2000	Right to privacy and confidentiality
Electronic Communications Act 2000	Cryptography & electronic signatures
Regulation of Investigatory Powers Act 2000	Authorised access to electronic storage and messaging; includes covert surveillance of staff or suspects
Data Protection Act 1998	Protection and use of personal information
Police and Criminal Evidence Act	Assuring auditable procedural and evidential information
Protection of Freedoms Act	Limits retention of biometric information held about innocent individuals
Copyright Designs and Patents Act 1998	Software piracy, music downloads, theft of Police data
Computer Misuse Act 1990	Unauthorised access to computers,

unauthorised modification of data

E.2 Data Protection Act

The Data Protection Act controls the processing of personal data about *living* people. Processing covers any use of the data including its storage and retrieval. In order to process data legally the processing must be in accordance with the eight data protection principles.

See the Data Protection Policy for further details.

E.3 Freedom of Information Act

The 2005 Freedom of Information Act grants a general right of access to records held by public authorities, including the Police, to encourage an attitude of openness. It facilitates public access to scrutinise organisations' decisions and working practises. The key features of the Act, as it applies to the City of London Police, are:

1. The public has a general right of access to all recorded information held by City of London Police. Subject to exemptions set out in the Act, a requester has the right to know whether a record exists, and the right to a copy of that record supplied in a format of their choice.
2. Every Police Force must adopt and maintain a Publication Scheme, listing what kinds of records it chooses to publish, how to obtain them, and whether there is a charge involved.
3. The Information Commissioner's Office will oversee the implementation and compliance with this Act and the Data Protection Act 1998. Freedom of Information requests are managed by the Information Access Manager.

E.4 Software Licensing

City of London Police uses software in all aspects of its business to support the work carried out by its employees. All commercial software is required to have a licence. Most non-commercial software has licence conditions[3]. City of London Police will not condone the use of any software unless correctly licensed; that is, that a valid licence has been purchased, or if free, that licence conditions are met in full.

Computer software must be purchased through IT Services and installed by a member of IT Services or appropriate arrangements may be made for a relevant member of the department to install the software. Acquisition exceptions may apply to covert or Computer Forensics departments, subject to legitimate licensing and suitable asset management.

Shareware, Freeware and Public Domain Software are bound by the same policies and procedures as all other software. No user may install any free or evaluation software onto City of London Police systems without prior approval from IT Services.

Users may not make copies of computer software owned or licensed by City of London Police for private use. Misuse of software in this manner can result in disciplinary action.

Managers must ensure that all policies and procedures within their area of responsibility are carried out correctly to achieve compliance with licensing standards.

3 Even free software will typically have a licence, such as the GPL, LGPL or BSD licence, which may impose restrictions upon the use and distribution of the software. Such licence conditions must be complied with if the software is to be used.

E.5 Force Information Security Policy (FISP) Compliance

E.5.1 Breaches and Discipline

All users who access or use any Force information, communications, computer or network system are responsible for using these resources in a professional, ethical and legal manner, compliant with this policy.

Where deliberate evasion of policies and procedures occurs, or where resources are utilised in unauthorised or inappropriate ways, this can result in withdrawal of IT privileges and/or disciplinary action, under the Force disciplinary policies or codes of conduct.

If abuse of IT systems does take place, the Commissioner reserves the right to regard those responsible for such abuse as being legally accountable.

Users found to have breached the Force Information Security Policy, may be subject to City of London Police's disciplinary procedure. Users who have broken the law may be subject to prosecution.

E.5.2 Seek Guidance

If you do not understand the implications of the Force Information Security Policy and this associated procedure manual or how it may apply to you, seek advice from:

- Your manager/supervisor
- The IT Service Desk
- The Force Information Security Manager
- The Information Management Board

F Personal Responsibilities and Compliance

ALL Users are to READ and RETAIN this section

F.1 Personal Responsibilities

All users are expected to be aware of the FISP and its contents, to operate within its guidelines and accept their responsibilities in assuring the integrity, availability and confidentiality of City of London Police and related information systems.

Users shall seek appropriate guidance and/or training from their line managers if there are any concerns over their ability to meet the FISP standards.

Non-employee users of City of London Police information systems, including contractors and agency staff shall be briefed, and if necessary trained, via their CoLP sponsoring managers, prior to being given access to City of London Police systems and information.

F.2 Acceptable Use Policy

The Force Acceptable Use Policy, which users must accept prior to being granted any access, must be read by all users. See Acceptable Use Policy on CityNet.

F.3 Email Retention

The email system is not to be used as a records management system. Emails must be stored with the associated parent record; all email will be automatically deleted at 12 months. It is the user's responsibility to store email in the most appropriate location and they are personally liable for the retention of material.

F.4 Information Classification

Users are expected to be aware of the relevant information classification, and respect the associated handling controls.

F.5 Information labelling, handling and disposal

City of London Police, in line with the national Police Service and ACPO requirements, have implemented HMG Government Protective Marking Scheme for appropriate information labelling and handling. It covers all formats of information, both physical and electronic. The labelling shall inform the user of the contents' value.

All staff, temporary workers and sharing partners shall be adequately informed/trained about GPMS procedures and have simple access to support documentation in order to assure appropriate recognition and handling of valuable information assets throughout their life-cycle.

Once National Guidance is available about the adoption of the new Government Security Classification (GSC), this information and training will be updated accordingly.

F.6 Sharing Police Information

Sharing of Police information external to City of London Police may not occur without formal authority and until due consideration for MoPI is in place. For example, all appropriate security must be in place, end-to-end, and any Data Protection compliance enforced and a formal Information Sharing Agreement (ISA) must be registered within the Force. All users must refer to the Information Sharing Procedure, associated with the Information Management Policy.

F.7 Remote Access / Off-site Use of Police Information by Staff

Where classified or personal information is to be accessed/used external to Police premises (e.g. on a Force laptop, at home or in partner agency premises), the user must ensure that FISP and Data Protection principles are maintained and the information is appropriately secured.

Staff may not connect their Police computer to other organisations' networks or systems without authority and appropriate security in place.

Prior to taking/using information off-site, authority shall be obtained. Information Asset Owners are responsible for ensuring that the appropriate use and security of the information asset is maintained when information is removed, or accessed externally, from City of London Police premises.

Staff working away from police premises must only use CoLP equipment to access systems and/or process data.

F.8 Removable Storage Devices and Media

Information valued above GPMS **RESTRICTED** or GSC **OFFICAL – SENSITIVE** may not be abstracted from its secure environment onto removable devices without appropriate authorisation. This will not be given without a written risk review. Any means of abstracting the data must maintain the appropriate security for the GPMS/GSC classification.

Only approved devices may be used. This applies to USB pendrives (or similar) and removable hard disks. When not actively in use, all removable media must be secured appropriate to its residual information GPMS / GSC valuation[4].

Police information may only be abstracted to removable devices for authorised business purposes. All removable storage devices must have approved encryption if removed from site.

F.9 Incident Reporting

Information Security incidents are varied and the implications and impact of an incident may not be fully understood at the outset.

4 For example, a suitably encrypted approved USB device might be suitable for CONFIDENTIAL information and, when locked, require protection as a RESTRITED asset.

Guidance on what is classified as a security incident is listed at Appendix F and also can be found here:

http://citymoss.colp/SiteDirectory/IMS360/SecurityMatters/SIR/default.aspx

Guidance on the reporting and management of a security incident is provided within this procedure.

G Access Control

G.1 General Procedures

G.1.1 Overview

Access to City of London Police's IT systems and information must be protected. Whilst different business applications have varying security requirements, these individual requirements must be identified through risk assessments that will establish appropriate controls to the IT/information systems.

It should be accepted that everything is generally forbidden unless expressly permitted, this should be the starting position for any access control policy for a specific information system.

The relevant information asset owners must ensure a process is in place to cater for exceptional cases, for instance in an emergency, where access is required to information through another User ID/password combination.

Access control rules should be supported by formal procedures and clearly defined responsibilities.

G.1.2 Scope of this Procedure

This procedure applies to everyone with any form of access to a City of London Police computer device or IT system.

G.1.3 User access management

User registration

The user should obtain authorisation from their line manager specifying the reasons for access. The line manager if satisfied that the request fulfils the relevant access control policy, will forward it to the relevant information asset owner for approval and implementation.

The relevant information asset owner must ensure that, before authorising access, the individual has received relevant training in the system, information security and data protection. The relevant information asset owner will maintain an accurate record of authorised users their access rights and training.

The relevant information asset owner should obtain a signature from every user indicating that they are aware of their rights, responsibilities and limitations with respect to the system.

The information asset owner will ensure that a formal user registration and de-registration procedure is in place, granting and revoking access to the appropriate information system. The level of access granted, should only be appropriate, to the business purpose and ensure it's consistent with the FISP.

Records must be maintained for the life of the system and disposed of in accordance with the Force Review, Retention, and Disposal Policy.

Privilege management

Access to special privileges, such as administrator rights, will be subjected to further controls. Allocation of privileges must be limited to as few persons as possible.

Privilege account identities should be kept separate from normal day-to-day user identities and should avoid obvious descriptors such as 'administrator' etc.

An authorisation process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorisation process is complete.

Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) can be a major contributory factor to the failures or breaches of systems.

User password management

Passwords are the most frequently used device for providing computer access control; other authentication mechanisms include IDs, smart cards and biometrics. Normally implemented by software, password systems range from the very simple to the highly complex and can be adapted to meet most needs. Because they are usually a first line of defence, they are particularly prone to attack and if broken, provide the easiest path into a machine.

The relevant information asset owner will ensure that systems incorporate a formal management process for controlling password access. Users must be required to keep passwords confidential. Initial, the user, preferably forced by the system, must change replacement or temporary issue passwords immediately. (See Appendix A - Secure use of Passwords)

Information asset owners are required to establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password.

A secure and effective means of issuing replacement or temporary passwords must be devised. Passwords shall not be sent by e-mail.

Review of user access rights

The relevant information asset owner will review access every 6 months and any redundant accounts deleted. Users who have not used their accounts for 6 months (3 months for privilege accounts) should be contacted and if necessary their accounts deleted. Accounts of users who leave the force must be deleted immediately or where individuals have been suspended the account must be disabled for the period of their suspension.

Privilege accounts will be subjected to greater scrutiny. Quarterly checks will be made to ensure that unauthorised privileges have not been acquired.

G.1.4 User Responsibilities

Password use

Users must ensure that their password is kept secret. Users should adopt best practice in the creation of passwords. Guidance is provided at appendix A of this procedure.

Users should be aware that any activity logged against their user identification is their responsibility.

Relevant information asset owners will adopt an effective password management system. The following controls, to ensure user authentication, are recommended.

1. Where possible passwords should only be issued to individuals. This will ensure accountability;
2. Users should be able to change their password;
3. A secure means of delivery for the initial password should be devised;
4. The initial password must be changed immediately, if not the account should be locked;
5. Previous passwords should not be reused;
6. Passwords must never be capable of being displayed on screen when being entered;
7. Password files should be encrypted;
8. Consideration should be given to providing duress alarm passwords for critical or sensitive systems or users.

Users must not disclose their passwords to others or use another user's User ID or password without authority.

Users must change their passwords if they suspect it has been compromised.

Passwords must not be written down.

Passwords must not be stored in macros or included in any automated log-on process.

Users who need access to multiple services/applications and are required to maintain multiple passwords may use a single quality password, but must exercise stringent security control of this password.

The Force Force Information Security Manager can provide further guidance on password design and usage on request.

Unattended user equipment

All unattended equipment must be subject to appropriate protection depending on its criticality or confidentiality. The relevant information asset owner will determine the appropriate level of protection for each piece of equipment. Users must be made aware of these requirements.

Terminals should be logged-out when not in use and the terminal lock (**ctrl, alt, del** then **Lock Workstation**) facility should be used if the terminal is left temporarily, however briefly.

Clear Desk and clear screen policy

All users should take into account the information classifications, legal and contractual requirements, and the corresponding risks and follow the Government Protective Marking Scheme controls as identified within this procedure for Asset Management and Classification.

The following controls are recommended:

1. Sensitive or critical business information, e.g. on paper or on an electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the work environment is vacated;

2. Computers and terminals should be left logged-off or should be protected by a screen and locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;
3. Incoming and outgoing mail points and unattended facsimile machines should be protected;
4. Unauthorised use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be prevented;
5. Documents containing sensitive or classified information should be removed from printers immediately.

A clear desk/clear screen policy reduces the risks of unauthorised access, loss of, and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

G.1.5 Duress alarms

It is considered appropriate to provide duress alarms for critical or sensitive systems or systems outside force buildings – this must be an agreed procedure between the relevant Information Asset Owner and the Chief Force Information Security Manager. The procedure will include specific use cases as well as determining appropriate counter measures.

G.1.6 Mobile computing and teleworking

Working on protectively marked assets away from official premises (remote working)

Remote working refers to work carried out in a work place that is away from force premises. Although remote working is widely associated with home working, the guidance in this section applies equally to other types of remote working, for example, in hotel rooms, at conference venues. It is assumed

that remote working is inherently less secure than when working in the controlled environment of official premises where the level of security in place is determined by the level of threat to that organisation and its assets.

When using mobile computing and communication facilities, e.g. smartphones, laptops, tablets, special care should be taken to ensure that force information is not compromised. This mobile computing section takes into account the risks of working with mobile computing equipment in unprotected environments.

Authorising remote working

Users have the authority to work away from force premises at the discretion of their line manager and can access information remotely where approved by the relevant Information Asset Owner – this is generally undertaken on a system basis rather than by specific users. However, when remote working on protectively marked assets, whether at home, in hotels or other places away from official premises, users are responsible for deciding on appropriate security controls within the environment. For example sitting in a hotel lobby accessing protectively marked assets where information can be easily viewed by others would not be acceptable, but accessing the material from within the hotel room would be.

Information asset owners are required to ensure that when they authorise remote access to the protectively marked information, appropriate physical, document and IT security controls are in place to provide required levels of protection before the access is permitted. In many cases such controls are unlikely to be onerous or limiting in their effect, but it should be recognised that it is rarely possible to provide the same level of security outside the work place as within. Users working from home should not be aware of the risk of 'advertising' that they work on official information at home.

When individuals remotely work on protectively marked information in the absence of appropriate security controls, including procedural controls and

other less formal safeguards, such as the presence of colleagues, there is an increased risk of deliberate and accidental compromise.

A remote worker also faces threats that are not necessarily directly linked to their employment. These include equipment theft and accidental or deliberate overlooking or eavesdropping. Continuous personal custody is rarely realistic and in some circumstances may be insufficient. For example, portable IT equipment is a highly attractive target for theft or robbery. IT threats are likely to be higher for the remote worker and could include:

- theft
- viruses
- hacking
- abuse of access rights
- interception - local and remote eavesdropping
- incorrect operation of transmission equipment
- denial of service

The level of physical security in official premises is often not realistic in the home or other remote work places. The vulnerabilities connected with remote working include:

- Weak physical defences;
- Poor IT discipline, for example, the use of insecure hardware and software, the use of unapproved network connections, introduction of malicious software to the remote worker and force systems;
- Insecure handling of documentation and electronic communications.

Exploitation of remote IT system vulnerabilities could lead to compromise of force systems. Whether remote working involves the use of IT, the preferred option, or simply the reading of documents, personal acceptance of responsibility for the protection of the assets involved is fundamental to good security practice.

The security procedures required for remote working include both technical and non-technical controls. Such controls will depend on the level of any protective marking, the requirements for business continuity and the degree to which IT systems are to be used for processing and transmitting information.

Before protectively marked assets are handled remotely, information asset owners should be satisfied that:

- Remote workers understand and accept their obligations in respect of the security controls necessary for the appropriate protection of the assets involved;
- All the necessary practical security controls and arrangements are in place;
- Where applicable, remote workers have been briefed on all security aspects of using IT equipment installed in the remote location.

Using your own software, computing equipment, or removable media

You must not use your own software, equipment, or removable media to process any protectively marked force information i.e. information that will attract a RESTRICTED, CONFIDENTIAL, SECRET, or TOP SECRET marking. NOT PROTECTIVELY MARKED work can be undertaken provided that you have the express authorisation of your line manager and the aggregation of such work would not attract a protective marking.

The use of privately owned computers, personal organisers, other technology or manual systems for the creation or processing of force 'owned' personal data is not permitted except where expressly authorised. Such activity will be conducted in accordance with the Force Information Security Policy, Procedures Manual and guidelines. Information asset owners must ensure this is clearly articulated in their relevant documentation.

Other than for diary, notes and contacts type information[5], all such authorisations for processing force information on personally owned equipment will be in writing through your line manager.

[5] Unless individual entries, or the aggregation of such information held, would attract a protective marking

Connections to the force computer or telecommunications networks will not be permitted for any personally owned computing equipment.

Remote working at home

Individual domestic circumstances and the level of protectively marked information involved will determine what physical security controls are needed and what is practicable to avoid compromise or embarrassment. It should be borne in mind that other users of the home may not share the home workers understanding of the need for discretion.

Mobile remote working (within the UK)

Accidental loss, overlooking or eavesdropping are the greatest risks when an individual is required to remotely work on protectively marked assets, e.g. while travelling. Mobile employees will often be at locations offering even lower levels of privacy than at home and it is essential that a high level of vigilance is maintained.

Normally, protectively marked assets should remain in the individual's personal custody and should not be set down in a public place. They should not, for example, be left in a cloakroom or on a train luggage rack while the individual goes for a meal. Where suitably protected, for example, by the use of a removable hard disk or an approved encryption product, portable computers are preferred to paper documentation.

Mobile remote working (outside the UK)

The threat to the remote worker overseas is, with few exceptions, greater than in the UK. In addition to the greater threat from deliberate theft of sensitive information, there may also be a greater threat from eavesdropping and interception. Individuals should take guidance from Special Branch and the Force Information Security Manager on the local threats.

The situation needs to be assessed on a country-by-country basis. It is not advisable, even in notionally friendly countries, to work outside secure premises without a full prior assessment of the risks.

Remote IT equipment, even when off-line, should be regarded as an extension of the work place system. It requires the same effective level of physical, technical and procedural security. Remote working is only permitted on dedicated force owned equipment with all the hardware, software and access control supplied and controlled by the force.

Transfer of Data (outside the UK)

Personal data shall not be transferred outside the European Economic Area, unless that country has an adequate level of protection for the rights and freedoms of data subjects.

Transfer of personal data to the United States is possible under the Safe Harbour arranged by the European Commission and the US Department of Commerce. This enables lawful transfer of data to US organisations that have signed up to comply with a set of data protection principles and to follow agreed guidance.

Otherwise, in determining what amounts to an adequate level of protection consideration will include the following:

- the nature of the personal data;
- the country of origin and destination;
- the purpose for which it is intended to be processed; and,
- the laws, and controls in force in the country in question.

The Data Protection Act (Sch. 4) provides for circumstances in which the above does not apply to a transfer. These include where the transfer has been consented to by the data subject or forms part of a contract with them, is necessary in the substantial public interest, the vital interests of the data subject or is in connection with legal proceedings.

Information asset owners should develop procedures for the assessment, authorisation and recording of transfers of personal data from their system to countries outside the European Economic Area.

The Recording and Dissemination of Intelligence Material Code of Practice and associated local procedures are recommended as a model of good practice in this area. Overseas transfers should be thoroughly risk assessed, documented and receive a Superintendent's authority.

Internet access

Internet connections should not be used for transmitting protectively marked information unless protected by approved encryption (at least 256bit).

There are a number of problems associated with connection to the Internet. The most damaging are viruses, spyware and hackers. Viruses, in particular, pose a threat to both the remote worker's own system and, where networked, to the department's or agency's on-line system.

Internet traffic may be routed anywhere in the world, regardless of the source and destination of the material; therefore great care must be taken, when sending personal data electronically, to ensure that the level of protection is adequate in the circumstances.

Remote access to force systems, if permitted and properly authorised, from abroad will amount to processing personal data in that country. Any such access must be subject to adequate protective measures by the information asset owner.

As a general rule, personal data, including photographs that are not already openly available should not be placed onto the Internet without the consent of the data subject.

Communications security

Intercepting communications can often be complex and difficult to achieve, but in the right circumstances can be relatively straightforward. Some simple rules can be applied to voice, fax, video and data transmissions to manage the risks.

Remote workers who are required to transmit information protectively marked CONFIDENTIAL and above should only use approved secure communications equipment. Further advice can be obtained from the Force Information Security Manager.

Transmission of documents and other assets

The carriage of protectively marked assets to, from and between official premises and remote work places should be conducted in accordance with the Government Protective Marking procedure provided within this document.

G.2 Technical Procedures

G.2.1 Network access control

Network Security

Network Security is concerned with the management and control of all the elements, that is, hardware, software, information and documentation contained within the network infrastructure. Connections between networks can be complicated by the differing security profiles of the two connecting networks, and the business requirements of the connection. Such connections should conform to the standard outlined in HMG standards, advice on which can be obtained from the Force Force Information Security Manager

Access to the network infrastructure should be limited to using procedural, physical and logical controls, and supported by network monitoring, accounting and audit functions.

All users of the network must be identified, and have their identity confirmed by a suitable authentication process. The creation of false users must be prevented by the protection of the associated management functions.

Passwords provide only one level of user authentication, and stronger mechanisms, such as Personal Identification Devices (PIDs), tokens and biometrics, should be used whenever highly privileged user-IDs are being

protected. Passwords that are stored for use in verification processes must be protected from disclosure, modification and replay. Normally storing passwords in an encrypted form does this. Wherever possible, passwords should not be transmitted across networks in their plain form.

Policy on use of network services

Users will only have access to the network and services they have been authorised, by the relevant information asset owner, to use.

Due to various technical changes to the UK public telecommunications networks over the last few years, including the phased switch to new and digital networks, the National Technical authority for Information Assurance (CESG) can no longer guarantee the protection of RESTRICTED data sent over these networks (e.g. PSTN, which includes GTN). This is largely due to the fact that the specified routes of calls cannot be guaranteed, and in some cases can be re-routed outside of the UK.

As a result there is an inherent increase to the risk of vulnerability and therefore potential compromise.

This is NOT an outright limit on RESTRICTED telecommunications on existing systems, but rather departments are now required to conduct a risk assessment to ascertain whether they can accept the risk.

Protectively marked information up to and including RESTRICTED may be transmitted via Government Assured Networks, this includes GSI, PNN, MOD, CJSM but **does not include** GOV.UK, GCSX or NHS.

The Criminal Justice Extranet (CJX) links forces and other criminal justice agencies to each other via a common backbone allowing for the exchange of e-mail and information within that community. It also provides a link to the Internet and other external networks for both e-mail, Web browsing and information access.

Inter-Force/Agency e-mail at the RESTRICTED level does not require encryption within the CJX or Government Assured Networks..

User authentication for external connections

The relevant information asset owner will determine the level of authentication-required dependent on the criticality or confidentiality of the information system. The risk assessment may determine that authentication is desirable even at the level of the force network or the application itself.

External connections will be subject to authentication consistent with the criticality or confidentiality of the information system concerned and not less than that prescribed in the Criminal Justice Network (CJX) Code of Connection and HMG S(E)N 99/1. The security policy for external connections to the force network, incorporating these standards, will be adhered to.

It is important to ensure that protectively marked information is transmitted only to the correct recipient. Originating callers should be satisfied that they are speaking to the intended recipient and that the recipient is authorised to receive that information. Verbal authentication would be usual for telephone calls and radio transmissions.

Facsimile transmissions should also include an authentication procedure since misdialling could transmit to an unauthorised machine, or faxes could be sent to an unattended device.

Remote diagnostics and configuration port protection

Physical and logical access to diagnostic ports will be securely controlled. A documented procedure to authorise and control access to a diagnostics port must be established.

Ports, services, and similar facilities installed on computer or network facilities, which are not specifically required for business functionality, should be disabled or removed.

Segregation in networks

The IS & T Director is responsible for the control of the force network and for ensuring that network services users and systems are segregated and securely routed.

Network partitioning is a powerful method of separating different communities and restricting user access within a network. It can be implemented in a number of ways:

Physical - this is the process of maintaining physically separate networks or infrastructures for different systems to ensure that one does not allow unauthorised access to the other. It provides the most assured overall security but at the price of duplicated equipment and administrative overheads.

Logical - there are a number of different techniques to achieve logical partitioning by:

- **Physical Address** The network defines a group of physical addresses, a subset of all the physical addresses on the network, as a community. It enforces controls on which physical addresses can be used to access other addresses within the community. Some networks can control which protocols may be used from a given address, for example, allowing e-mail but not file transfer.
- **Identifier** The network recognises different user communities by the user identifier. Such communities are often known as a Closed User Group, and tend to be implemented by vendor dependent applications.
- **Encryption** All users of a particular community (sometimes called a COI or Community of Interest) or sub-network are equipped with encryption facilities, thereby creating a Virtual Private Network or "Tunnel". Distributing keys only to the authorised members of the community enforces the partition. This provides very effective partitioning.
- **Routers** These are network communications devices allowing, or barring, packets from being transmitted across sub-network boundaries. Their

routing tables can be set up to control access between LANs according to either the sender's or recipient's network address. These devices are not normally considered by their vendors to be security devices, but communication devices for the efficient implementation of network infrastructure.

- **Secure Gateways** Commonly known as Guards or Firewalls, act as bridges or routers that perform a greater level of security checking before passing on data packets across network boundaries. They act as barrier devices, and are often implemented where a trusted network interfaces to an un-trusted network. It is important to realise that a Firewall is a collection of trusted devices forming an architecture that provides Firewall functionality.

Security of network services

The Technology Section will maintain a clear description of the security attributes of all network services used by the force.

Network connection control

For guidance on how to determine the nature and level of IT security controls required depending on the differing security profiles of the connecting networks – contact the Force Information Security Manager who can advise about connecting business domains. An approved circuit may be used to pass information protectively marked up to and including a specific level, normally RESTRICTED, without being encrypted.

An 'approved circuit' is a landline, either fibre-optic or wire, and associated terminal equipment, to which certain electro-magnetic and physical safeguards have been applied in order to prevent unauthorised interception. Because such circuits are usually under close control, the risks are reduced and higher protective markings can be conveyed without encryption.

The incorporation of controls to restrict the connection capability of the users may be required by the access control criteria for shared networks, especially those extending across organizational boundaries.

G.2.2 Operating systems access control

Automatic terminal identification

Relevant information asset owners should consider automatic terminal identification to authenticate connections to specific locations and to portable equipment depending on the criticality or confidentiality of the system. This risk assessment shall be documented and reviewed periodically.

Terminal log-on procedures

Access must only be permitted through a secure log-on procedure. The following controls are recommended:

- System or application identifiers should not be displayed until the log-on has been successfully completed.
- Display a general notice warning users that authorised users must only access the system.
- Not provide help messages that would assist an unauthorised user to gain access.
- Limit the number of failed log-on attempts to a maximum of three then disconnect and provide no assistance. Where possible user accounts should be locked after three unsuccessful attempts to log-on. If this is not possible a minimum ten-minute time delay should be introduced prior to any further attempts to log-on being permitted. Record all failed attempts in an audit log.
- Where possible the minimum time limit for log-on should be at least one minute and the maximum time permitted should be three minutes. Outside these time limits the log-on procedure should be terminated.

Where possible the following information should be displayed upon a successful log-on:

- The last time and date of a successful log-on.
- Details of any unsuccessful attempts to log-on since the last successful log-on.

User must report, through their normal management channels, any unusual or suspicious successful or failed log-on attempts.

User identification and authentication

The user naming standards for User ID's will be based on Warrant card numbers for Officers and the payroll numbers for other members of staff. Single sign-on is recommended, this will reduce the opportunity, by the presentation of further sign-on screens, for unauthorised users to attempt to access other systems for which the authorised user has no permissions.

Password management system

See Appendix A - Secure use of Passwords.

Utilities

Control must be kept of utility programs so that they cannot be used to deliberately or inadvertently corrupt data, systems or software. System users must not load or use utility programs. Staff responsible for diagnostic across the enterprise will document procedures to ensure that only necessary utilities are maintained and that only authorised persons can access and use them for specific purposes. Utility programs should be removed when not in use. An audit log of use must be maintained and may be required in any subsequent investigation where digital Forensic Evidence is required.

Terminal time-out

Force terminals must be configured to time-out after a set period. The period of time should be adjustable depending on the confidentiality or criticality of the system. As a maximum threshold, screens should revert to the log-on screen after ten minutes.

Limitation of connection time

Where available system access will be limited to connection times to the work pattern of individual users – providing additional security for high-risk

applications. Attempts to log-on outside the specified period should be logged and create an alert.

G.2.3 Application and information access control

Information access restriction

The relevant information asset owner will ensure that access to information is in accordance with the access control criteria for that information. Users will only be accorded the minimum rights necessary to perform their role.

Sensitive system isolation

Systems processing information protectively marked at CONFIDENTIAL or above, or other critical systems, will where possible, have a dedicated environment and only share resources with trusted applications. Sharing must be agreed in advance with the Head of Technology and the Force Information Security Manager and extra security controls considered commensurate with HMG standards. Relevant advice can be obtained from the Force Information Security Manager.

H Asset Management

H.1 General Procedures

H.1.1 Accountability and inventory of assets

Accountability

The following are examples of the assets of the force which require protection:

- Personal data relating to the user of any force service must be protected against loss, damage, or unwarranted disclosure in line with the relevant data protection and privacy legislation;
- Corporate information base of the force in general must be protected against loss, unwarranted disclosure, or introduction of erroneous content;
- Force information infrastructure (comprising the applications and delivery platforms) must be protected against threats to its availability and integrity of the service offered;
- Authentication credentials must be protected against forgery or unwarranted use;
- Objects that represent monetary or other value must be protected against fraud. Some of the force transactions are likely to result in cashable orders that must be properly controlled, some may relate to the delivery of goods that can be misappropriated.

Inventory of assets

All assets should be clearly identified and an inventory of all-important assets drawn up and maintained.

The information asset owner will draw up inventories for all relevant information assets.

Inventories will include:

- Information Assets – databases, system documentation, user manuals, business continuity plans, etc.
- Software Assets – application software, system software etc.
- Physical Assets – computer and communications equipment, specialist equipment (power supplies, air conditioning units etc.)
- Information asset owners should conduct an audit every two years

The process of compiling an inventory of assets is an important prerequisite of risk management.

H.1.2 Information Classification

Classification guidelines

Information and related IT assets have a value. Information asset owners should know what assets they hold in order to make best use of them, to manage them effectively and securely, and to conform to legal requirements. The value of assets plays a part in determining the associated security requirements.

Classifications and associated protective controls for information should take account of force needs for sharing or restricting information and the impacts associated with such needs.

The value of information is based on its protective marking. However, even information having no protective marking will have value, expressed in terms of the time, cost or effort of replacing it if lost or corrupted, and it will merit inclusion in an asset valuation exercise.

The costs of losing and replacing such assets need to be considered by information asset owners when developing security policies and carrying out risk assessments.

Protectively Marking Information

‘Protective Marking’ is the method by which the originator of an asset, indicates to others, the levels of protection required when handling the asset in question, in terms of its sensitivity, security, storage and movement both within and outside the originator’s own department or force and its ultimate method of disposal.

Security controls are required where there is a risk that the deliberate or accidental compromise of assets will interfere with the effective conduct of the Force’s business.

An effective system of control is essential for the protection of protectively marked and other valuable documents against compromise. Such a system must allow information asset owners and their contractors to know:

- What protectively marked documents they hold;
- What level of protection it must be given;
- Where it is held;
- Who is authorised to see or use it and, at the higher levels of protection;
- Who has had access to it or has used it in the past.

Protectively marked or other valuable assets are at risk during transit from accidental or deliberate compromise. To protect such assets when in transit the means of carriage must be reliable, the packaging robust, and the attractiveness, identity and source of the assets concealed under plain cover. Where higher levels of protectively marked assets are involved, a system of audit must be built in to track such assets and to reveal any actual or attempted tampering.

For further detailed information see Protective Marking & Handling in this procedure.

I Communications and Operations Management

I.1 General procedures

I.1.1 Documented operating procedures

All information systems must be subject to security operating procedures (SyOPs). Such a procedure will comply with this framework, the relevant system security policy (SSP) and exert whatever additional security controls a local risk assessment deems necessary. Careful consideration must be given to the recommendations of this framework and the results of any risk assessment. All decisions must be justified and documented.

The security operating procedures will be owned, managed, and maintained by the relevant information asset owner. The SyOPs must be readily available to all users at all times for reference. The relevant information asset owner will undertake responsibility for auditing the system to ensure compliance with this procedure, relevant system security policies and their own security operating procedures.

Auditing policy, practice, procedure and results will be fully documented and subject to quality assurance checks by the Force Information Security Manager. The policy will be reviewed annually. The Force Information Security Manager must approve all security operating procedures.

I.1.2 Security of system documentation

System documentation can provide valuable information to unauthorised persons attempting to access systems. Relevant information asset owners must ensure that distribution of such material is minimised. System documentation must be kept securely locked away when not in use. Sensitive system documentation held on computer must have additional access controls applied. Effective audit procedures must be established. These procedures must be regularly reviewed and tested by the relevant information asset owner and commensurate with the requirements of the Government Protective Marking Scheme.

I.1.3 Operational Change control

In order to minimise the corruption of applications there must be strict control over the implementation of changes. The relevant information asset owner authorises and oversees the implementation of locally owned system changes. Changes to centrally owned resources will be implemented and controlled by the Technology Department.

Change Control procedures should ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of the system that are necessary for their work, and that formal interdisciplinary agreement and approval for any changes are obtained. Changes to facilities and systems should be controlled. The responsibility for controlling changes to the facilities lies with the relevant information asset owner.

The following items should be covered:

- Identification and recording of any changes to the system.
- Planning and testing of changes.
- Analysis of the potential impact of such changes.
- Approval procedure for proposed changes.
- Communication of change details to all relevant persons.
- Procedures and responsibilities for aborting and recovering from unsuccessful changes.

I.1.4 Segregation of duties

Relevant information asset owners will ensure duties and areas of responsibility are segregated in order to reduce opportunities for negligent or unauthorised modification or misuse of information or services. This segregation of duties will be documented as part of security operating procedures.

Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered. It is important that security audit remains independent. The possibility of collusion should not be forgotten when designing the controls.

I.1.5 Separation of development and operational facilities

Developmental activity must, where practicable, be kept separate from the live system. Any changes to the operational system will be subject to documented change control procedures, as described above.

I.1.6 Third party service delivery management

The relevant information asset owner must identify any risks and adopt appropriate control measures prior to any external service management being utilised. The contract with the external provider will specify the necessary measures needed to ensure that the relevant information system retains its confidentiality, integrity and availability.

The force should ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disasters.

I.1.7 Protection against malicious software

No unauthorised software is permitted on any device connected to the City of London Police Network.

All access to email resources must be undertaken via an approved force gateway, as accredited by the force information security manager, using only those email programs supplied by the IT department.

All access to Internet resources must be undertaken via an approved force gateway, as accredited by the force information security manager, using only those email programs supplied by the IT department.

Any external force connection is subject to monitoring.

The IT department will maintain anti-virus software across the force. No device is permitted to connect to the force network without appropriate anti-virus controls.

I.2 Exchanges of information and software

Any exchange of information with external organisations must be subject to a formal protocol. Such a protocol will address responsibilities and liabilities, exchange procedures, data protection act considerations, audit, information classification and handling, and information security in general.

I.2.1 Security of media in transit

Security of information assets in physical transit must be consistent with the protective marking of the information.

I.2.2 Electronic commerce security

Electronic commerce will not be entered into without the prior express approval of the Technology Programme Board.

Should any such activity be approved, in the future, it must first be supported by a security policy designed to protect the confidentiality, integrity and availability of force information. Consideration must also be given to protecting the force from fraud, contractual disputes and unauthorised disclosure or modification of information.

I.2.3 Publicly available systems

Information must not be made publicly available on force information systems unless expressly approved by the relevant information owner. Published information must be protected from modification. (see Intranet Policy)

Due to various technical changes to the UK public telecommunications networks over the last few years, including the phased switch to new and digital networks, the National Technical authority for Information Assurance (CESG) can no longer guarantee the protection of RESTRICTED data sent over these networks (e.g. PSTN, which includes GTN). This is largely due to

the fact that the specified routes of calls cannot be guaranteed, and in some cases can be re-routed outside of the UK.

As a result there is an inherent increase to the risk of vulnerability and therefore potential compromise.

This is NOT an outright limit on RESTRICTED telecommunications on existing systems, but rather departments are now required to conduct a risk assessment to ascertain whether they can accept the risk.

Digital mobile phone services based on pan-European standards, DCS 1800 and GSM offer some degree of protection to calls made on them. Radio transmissions between the handset and the base-station are encrypted; however when a call is passed onto another base-station within the cellular network or to the PSTN it is in clear.

I.2.4 Internet usage and protective marking

Information protectively marked CONFIDENTIAL or above must not be transmitted over the Internet, or similar networks. Information protectively marked RESTRICTED may be transmitted over the Internet, or similar networks, provided that an appropriate grade of encryption is used.

Information asset owners making use of Internet or similar services are reminded that this is an area of rapid technological change, attracting considerable public attention, with the prospect of appreciable embarrassment should mishaps occur. There are no 'fit-and-forget' solutions to security in this area; new technical threats to security appear frequently, and some may defeat current protective controls. The continued effectiveness of any local protective controls must be monitored regularly. For the common good, security incidents must be reported promptly, and any corrective action recommended should be promptly applied.

I.2.5 Other forms of information exchange

Information is exchanged in a variety of ways such as telephone, fax, video, etc. Great care must be taken to ensure that information exchange and

disclosure takes place only in accordance with Force instructions. Prior to disclosure personnel should ensure the identity of the recipient and that they are entitled to receive such information. Disclosure of personal information must adhere to the provisions of the Data Protection Act. Any information exchange with an outside agency must be subject to a protocol as described above.

Voicemail systems are inherently vulnerable to hacking and therefore should never be used for protectively marked messages.

I.3 Technical procedures

I.3.1 System planning and maintenance

Capacity planning

Relevant information asset owners will ensure that adequate processing power and storage are available to meet projected demand. The Head of Technology is responsible for capacity planning in respect of centrally owned IT resources.

System acceptance

System or project managers will document the acceptance criteria for new information systems, upgrades or new versions. Any new system, upgrade or version must be tested prior to acceptance or installation.

I.3.2 Housekeeping

Information back –up

The relevant information asset owner is responsible for agreeing with the IT department the appropriate settings for the backup of information. Frequency will depend on the criticality or confidentiality of the data.

The relevant information asset owner should ensure that the IT department test the integrity of the backup by performing the restore operation on an agreed basis – at least once a year.

All backups and statutory data must be stored in a manner consistent with its criticality or confidentiality. Wherever practical, storage of backup media should always be in a building other than that where the original data is located.

The IT department is responsible for the management and maintenance of the backup solution including the engagement with third party suppliers where backup of data is managed under contract.

Relevant information asset owners must determine and document a policy of data retention, weeding and archiving consistent with the requirements of the Management of Police Information.

Fault logging

All faults to force systems shall be reported to the Technology help desk. Faults to other systems will be reported to the relevant information asset owner. All faults will be logged and corrective action documented. Fault logs will be reviewed regularly to ensure all faults are dealt with and that security has not been compromised. Reviews will be documented; frequency will be determined and documented, based on the criticality or confidentiality of the system.

I.3.3 Network management

Network controls

The IT department will be responsible for the operation of the network and will ensure data security controls are established to prevent unauthorised access. Particular care must be taken with regard to protecting data passed over public networks.

The IT department will establish effective procedures to counter any breaches of security. All breaches or suspected breaches of security must be reported to the Force Information Security Manager.

I.3.4 Media handling and security

Management of removable computer media

Relevant information asset owners will document procedures regarding removable computer media such as disks, tapes and printouts. Media should not be removed without express permission. Security measures consistent with the criticality and sensitivity of the data should be applied.

Information handling procedures

Relevant information asset owners should determine a media handling and storage policy commensurate with the relevant protective marking baseline standards. Media includes not only removable computer disks, but also, mail, telephone and fax services, photocopiers, post (internal and external), video, voice mail, paper and any other means of recording information, electronically or mechanically.

The policy should determine the handling, labelling and secure disposal of all types of media, and establish a documented audit trail and local audit regime. The purpose of these procedures will be to ensure that information assets are not lost or damaged.

Security of system documentation

System documentation should be stored securely with appropriate access controls limited to authorised users only.

I.3.5 Monitoring system access and use.

Event logging

Once an information system is in use, it is essential for security management personnel to be able to track the way in which the system is used and to ensure that security controls are effective in practice. Specific events and details relating to the operation of the system and its security controls must be recorded for subsequent inspection and analysis. More than other forms of security, information security measures are liable to be influenced by

technology developments and re-configuration, and regular audit review is essential.

The following events should be logged and retained for at least one year:

- Changes to user or group management.
- Log-on and log-off (except for successful log-ins).
- Changes to security policy.
- The use of privileges and restart or shutdown of the system.
- Archiving and deletion of audit logs.

Information logged should include; User ID's, date, time, type of event, files and records accessed, programs, utilities, devices used and terminal identity and location.

Operating systems generally record both successful and unsuccessful events. However, it is the case that the details of unsuccessful events can be more revealing Operating systems are capable of recording vast amounts of detailed information about a wide range of system events. However, most operating systems have facilities to allow the system manager to define and select which events are to be recorded in the audit log as security audit messages. Generally, for the purposes of system security, it is the recording of exceptional events that is required and will be of greatest interest in determining compliance with the System Security Policy.

Monitoring system use

The level of monitoring will depend on the confidentiality or criticality of the system and the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations.

Relevant information asset owners must inform users that their activities are being monitored.

It is important to establish what are the normal and acceptable patterns of use of your system before you can recognise potential security problems. Once

this is done procedures should be established to regularly review the audit log. Consideration should be given to monitoring the following:

- The number of unsuccessful log-ons.
- Accounts with privileged facilities.
- Access failures.
- Trends in unsuccessful log-ons.
- Out of hours usage
- Usage trends of specific accounts.
- Tracing of selected transactions.
- Trends in reports printed.

The audit log should periodically be analysed. The size, number of users and amount of system use will help determine how often this should be done. The most common type of report is a brief daily listing of selected events that is created from running a batch job every evening before midnight. It is important that such reports are reviewed as soon as possible in order to gain early warning of any system security breaches.

The relevant information asset owner must establish and document an effective monitoring regime. The Force Information Security Manager who will conduct quality assurance checks of the audit records supplied by the relevant information asset owners, and report the findings to the Head of the Professional Standards Unit must approve this regime.

Clock synchronisation

Computer clocks must be synchronised to ensure the accurate recording of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.

Computer and communication devices that have the capability to operate a real time clock must be set to local standard time.

There must be procedures to check and correct time variations including change over to and from summer time.

J Protective Marking and Handling

The originator of a document (whether in hard copy or electronic form) should consider whether it needs a protective marking. Applying a protective marking to a sensitive information asset indicates to others the appropriate level of protection and security controls required to protect it against compromise.

When applying protective markings the originator should bear in mind that security controls can be costly; the higher the level of protective marking, the greater the cost of protective controls it attracts. Consequently, it is important to take into account the level of access required and the implied cost of the protective controls that should be given when applying a specific protective marking.

Applying too high a protective marking to an asset can inhibit access, lead to unnecessary protective controls and impair the efficiency of Force business. Conversely, applying too low a protective marking can put assets at risk of compromise, since the appropriate controls may not be in place.

J.1 Staff Responsibilities

Line managers are responsible for ensuring that individuals correctly mark sensitive assets.

Only the originator can protectively mark an asset or change its protective marking, though holders of copies may challenge the level of protective marking applied. Where agreement cannot be reached, the information asset owner will determine the protective marking. Final arbitration rests with the Force Information Security Manager. All challenges to a protective marking and decisions taken must be recorded and retained with the information to be protectively marked.

Where the originator is no longer available, his/her successor becomes responsible. Where a successor cannot be traced, the holder of a copy document may change its marking only after consultation with all other addressees.

When assessing the value of an asset it will be necessary to consider the direct and indirect consequences of compromise in relation to a breach or loss of:

- Confidentiality – the restriction of information and assets to authorised individuals.
- Integrity – the maintenance of information systems and physical assets in their complete and proper form.
- Availability – the continuous or timely access to information systems or physical assets by authorised individuals.

J.2 Protective Marking Identifiers[6]

A comprehensive list of the criteria covered by the system is at Appendix B, but the following extract covers most situations relevant to police work:

J.2.1 NOT PROTECTIVELY MARKED

The compromise of this material would not be likely to have the impact warranting the security measures mandated for protectively marked material, but the absence of a protective marking does not necessarily mean that the material may be made freely available.

J.2.2 PROTECT

Impact level 1

The compromise of this material would be likely to cause:

- No impact on life and safety;
- Minor disruption to emergency service activities that require reprioritisation at local (station) level to meet expected levels of service;
- No impact on crime fighting;
- No impact on judicial proceedings;

[6] The Government Protective Marking Scheme (GPMS) is being replaced by the Government Security Classification. Although the Government have gone live with GSC in April 2014 the Police service have yet to adopt it.

Impact level 2

- Inconvenience or cause discomfort to an individual;
- Minor disruption to emergency service activities that requires reprioritisation at area / divisional level to meet expected levels of service;
- Minor failure in local Magistrates Courts.

NOTE: Not to be used for operational issues; Must be accompanied by a "Descriptor" (e.g. PROTECT – STAFF)

J.2.3 RESTRICTED

The compromise of this material would be likely to:

- Cause substantial distress to individuals;
- Make it more difficult to maintain the operational effectiveness or security of the UK or allied forces;
- Prejudice the investigation or facilitate the commission of crime;
- Impede the effective development or operation of government policy;
- Breach proper undertakings to maintain the confidence of material provided by third parties;
- Breach statutory restrictions on disclosure of material (e.g. unauthorised disclosure of personal data contrary to the Data Protection Act);
- Disadvantage government or the Force in commercial or policy negotiations with others.

J.2.4 CONFIDENTIAL

The compromise of this material would be likely to:

- Prejudice individual security or liberty;
- Cause damage to the effectiveness of valuable security or intelligence operations; or
- Impede the investigation or facilitate the commission of serious crime.

- Seriously impede the government policies
- Shut down or otherwise substantially disrupt significant national operations.

J.2.5 SECRET

The compromise of this material would be likely to:

- Threaten life directly, or seriously prejudice public order, or individual security or liberty or
- Cause serious damage to the continuing effectiveness of high valuable security or intelligence operations.

J.2.6 TOP SECRET

The compromise of this material would be likely to:

- Lead directly to widespread loss of life; or
- Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.

J.3 Handling

See Appendix B for a full description.

J.3.1 RESTRICTED AND CONFIDENTIAL

Baseline security measures are sufficient.

J.3.2 SECRET

All material protectively marked SECRET must be recorded on movement sheets when it is received, despatched, destroyed, or moved to other locations or branches.

As an added measure, originators must number each copy and record them in a register.

J.3.3 TOP SECRET

All TOP SECRET material must be recorded on movement sheets when it is received, despatched, destroyed, or moved to other locations. You must keep copies of material to the minimum necessary. As an added measure, originators must number each copy and record them in a register.

A register for recording the movement of SECRET and TOP SECRET material must be maintained by all units. As a minimum this register must record the date out/returned, addressee, seal number and the name of person conveying the material.

J.4 Physical Storage

J.4.1 Storage Rules

Protectively marked material should be stored in a secure environment, which is defined as a barrier, or combination of barriers, providing protection commensurate with the risk of compromise.

RESTRICTED material should be protected by one barrier internal to the building e.g. a locked container.

CONFIDENTIAL material should be protected by two barriers internal to the building e.g. a locked container within a locked room.

SECRET or TOP SECRET material should be stored in approved security containers.

Effective key control systems must be in use to ensure access is limited to those who need to access the particular material and to provide a record of keys issued, where appropriate.

J.4.2 Destruction

Whilst the current “Blue Bins” are commonly referred to as confidential waste bins this should not be confused with the Protective marking of CONFIDENTIAL. The Blue Bins have been security assessed as being acceptable for information to PROTECT.

PROTECT documents must be torn by hand into a number of pieces before being placed into the “Blue Bin”

RESTRICTED documents must be shredded prior to being placed within the “Blue Bin”.

CONFIDENTIAL documents must be shredded using a crosscut shredder. The Force Information Security Manager can provide advice on the purchase of shredders.

SECRET documents may be destroyed using a cross cut shredder configured to the government standard (60 sq. mm).

For advice on the destruction of TOP SECRET documents and guidance on all aspects of physical protection contact the Force Information Security Manager.

J.5 Movement of Protectively Marked Material

J.5.1 CoLP Personnel

If protectively marked material is being carried in a public place, it must be kept under cover with no outward indication of the contents. The material must not be left unattended and outside the immediate direct control of the carrier at any time.

When carrying protectively marked material, all items must be treated according to the highest marking.

TOP SECRET documents must only be carried by a person having a security clearance appropriate for unsupervised access to them. A receipt must be

obtained each time a TOP SECRET document changes hands unless it is within an area where other measures have been specifically agreed.

J.5.2 Internal Despatch Service

When sending protectively marked documents within the CoLP via the internal despatch service the following rules apply:

RESTRICTED: Use a sealed envelope, with the protective marking shown on the envelope. Transit envelope may be used for internal mail, but the flap must be sealed with the appropriate label.

CONFIDENTIAL: Use a new sealed envelope, with the protective marking shown on the envelope then place this within another envelope with no protective marking shown. Transit envelopes must not be used for CONFIDENTIAL documents.

SECRET and TOP SECRET documents must NOT be sent via the internal despatch service.

J.5.3 Royal Mail/Courier Services

When sending any external mail a return address or 'PO Box' number must be shown on the reverse of the envelope.

When sending protectively marked material within Great Britain by Royal Mail or courier the following rules apply:

- RESTRICTED material may be sent by ordinary post. It must be sent in a sealed envelope with no protective marking visible (except PERSONAL, when appropriate).
- CONFIDENTIAL material must be sealed in an envelope showing the protective marking and addressed to a named individual, or specific appointment. This envelope should be sealed within a second envelope, suitably addressed and with a return address or PO Box number on the reverse, but with no indication of the protective marking.

- SECRET and TOP SECRET documents must not be sent via the Royal Mail or courier service.

More detailed rules on the movement of protectively marked material are shown in the table at appendix B.

K Data Breach and Incident Management

K.1 Definition of an Information Security Incident

An information security incident is defined as any event that has, or could have, resulted in the loss of, or damage to, or unauthorised disclosure of, any City of London Police information asset.

The Force Information Security Manager (ISO) is responsible recording, examining and making recommendations to prevent such incidents reoccurring.

Information System Owners are responsible for collating details, taking immediate appropriate action to prevent a reoccurrence, immediately reporting the incident to the Force Information Security Manager (ISO) and if relevant the Technology section. A report outlining any information security issues must be sent to the Head of Professional Standards (HoPS) and the Head of Technology (HoT) for consideration of appropriate countermeasures.

Information system assets include, but are not limited to:

- Information assets - Databases, system documentation, user manuals, business continuity plans fall back arrangements etc.
- Software assets – application software, system software
- Physical assets – computer and communication equipment, specialist equipment (power supplies, air conditioning units etc.)

A security breach could result in a variety of different consequences, which may include:

- jeopardising national security;
- frustrating the apprehension or prosecution of offenders;
- impeding the prevention or investigation of offences;
- facilitating the commission of crime;
- distress, injury or death to individuals;
- disruption of operations or other activities;

- loss, destruction or unauthorised disclosure of information;
- invasion of privacy;
- legal obligation or penalty;
- financial loss;
- damage to the reputation or integrity of the City of London Police; or
- embarrassment to the Service.

Reportable incidents under the Information Security Incident Reporting Scheme (ISIRS) include compromise or potential compromise to the confidentiality, integrity and availability of City of London Police assets, such as:

- accidental or deliberate unauthorised destruction, loss, modification or disclosure of information;
- deliberate, unauthorised or catastrophic (in terms of business impact) unavailability of systems;
- unauthorised access to information, IT, radio and telephone equipment/systems or protectively marked equipment;
- misuse or unauthorised use of information, IT, radio and telephone equipment/systems or protectively marked equipment;
- malicious damage to IT and radio equipment/systems or protectively marked equipment;
- malicious software (virus);
- theft of information (plans, files, papers, floppy disks, etc.), IT equipment or protectively marked equipment;
- any other event which affects security.

K.2 Reporting Security Incidents

Information security incidents must be immediately reported to the ISO. All malicious software (virus) incidents must also be reported to the IT Helpdesk immediately.

Where appropriate, information security incidents involving an unrecoverable fault or failure of IT equipment must be reported to the IT Helpdesk.

When a virus is detected on an information system, the information asset owner / administrator will report the infection in accordance with the relevant System Security Policy (SSP), and their own Security Operating Procedures (SyOPs). If the virus is discovered by the Technology Unit they will contact the relevant systems owner / administrator and the ISO.

All personnel must be encouraged to report any perceived information security weaknesses through their line management to the ISO.

It is not normally necessary to report one-off minor incidents, e.g. where a user has trouble keying in a password. What is a minor incident in one set of circumstances may be a major incident in another and judgement must be exercised when deciding whether a report should be made. For example, if a user accidentally switches off the power to a computer, it is unlikely to cause serious disruption to business unless the computer is used as a file server for a network. If, however, the power supply to the Command & Control system was similarly interrupted it would be likely to constitute a major incident.

Some information security incidents are handled through other mechanisms and the following provisions apply:

- Police Property & Equipment: theft and criminal damage are reported as crimes. However, the theft or damage, or unauthorised disclosure of information, of IT equipment or protectively marked equipment are additionally reportable under the ISIRS.

- Physical Security incidents: Reported to the Heads of Departments and Divisions are also reportable under the ISIRS. For example, burglary or trespass on City of London Police premises containing information assets.
- Equipment Security (Information Systems): unavailability of force systems are normally dealt with under serviceability arrangements between the information asset owner and the relevant service provider. However, deliberate or catastrophic (in terms of business impact) unavailability are additionally reportable under the ISIRS.
- Personnel Security (Warrant Cards, Civilian Support Staff Passes and other Security Passes): rules covering the loss or theft of these are detailed in Force Orders and are not therefore, reportable under the ISIRS.
- Personnel Security: corruption, dishonesty and unethical behaviour is dealt with through Police or Civil staff disciplinary procedures. However, if this is connected with the use of information system equipment such instances are additionally reportable under the ISIRS.

Unauthorised attempts to investigate any suspected security weakness could be interpreted as a disciplinary and/or criminal offence.

K.3 Incident Handling

On being notified of an information security incident the ISO will initiate incident handling procedures. These procedures ensure a uniform and consistent response to incidents by incident management, escalation where necessary and the identification of countermeasures to avoid recurrence.

The major concern during an information security incident evaluation is not to attach blame to an individual, but to improve and maintain security and to rectify any shortcoming.

The ISO will offer advice, guidance and instructions to the reporting officer who will ensure local compliance. If you breach any instructions you may be committing a serious disciplinary and/or possibly a criminal offence.

The ISO collates information from security incidents. This information forms the basis of a report for the analysis of trends, security weaknesses and appropriate countermeasures

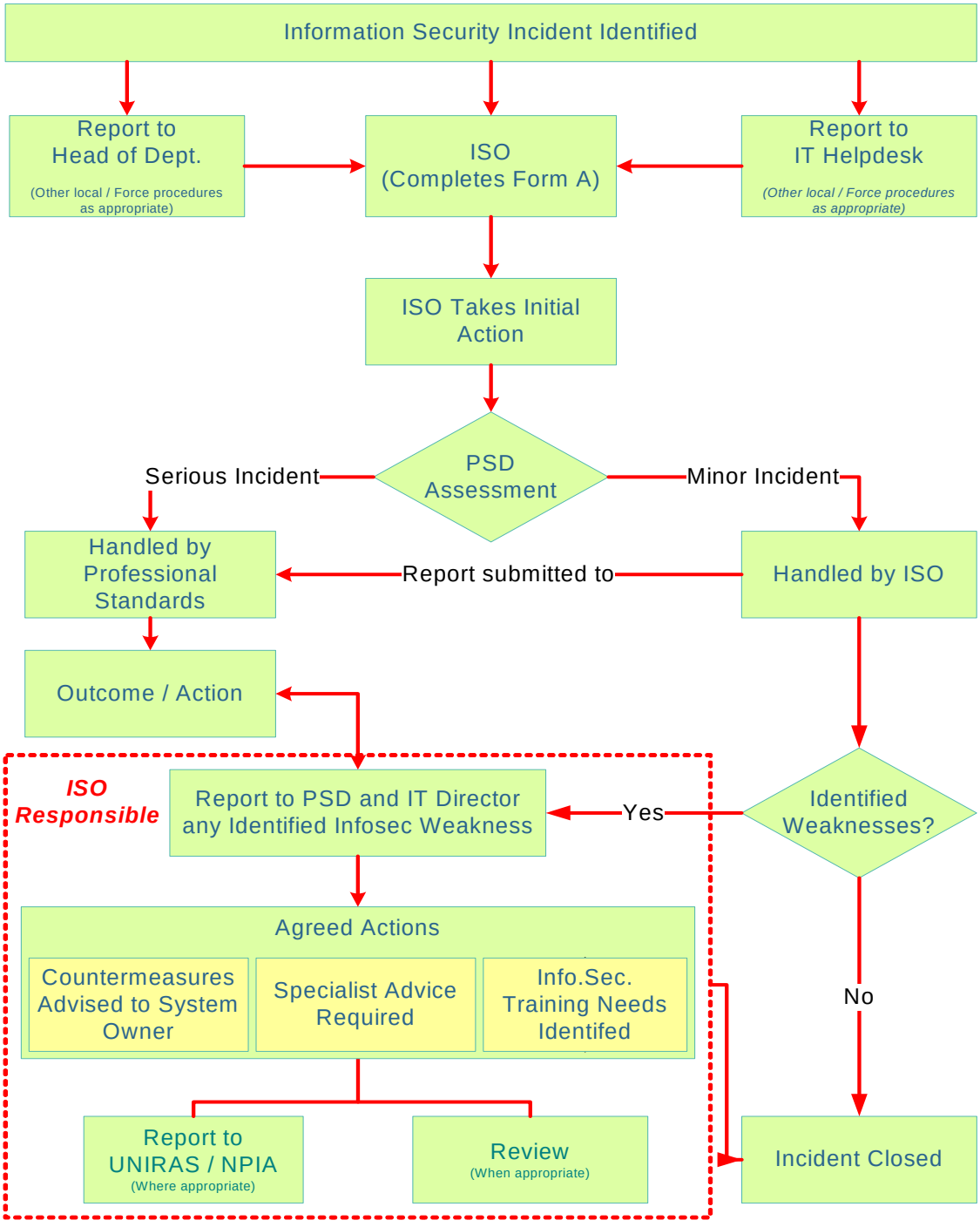
Where appropriate, if the ISO identifies training needs that have arisen as a result of an incident the ISO can offer specialist guidance to divisions and departments in dealing with this requirement.

The ISO will forward details of all relevant security incidents to the National Police Information Risk Management Team via PoLWARP for inclusion in the government's Unified Incident Reporting and Alert Scheme (UNIRAS).

The ISO receives Security Alerts and Briefing Notes from Centre for The Protection of National Infrastructure (CPNI). These are then forwarded to appropriate individuals.

In accordance with the PNC System Security Policy, Code of Connection Volume 1, the ISO shall forward details of any security incident involving PNC data to the Home Office Force Information Security Manager.

Information Security Incident Management Scheme Flowchart



L Internet and Email

L.1 Purpose

This procedure informs all users (Police Officers, Civilian Staff, members of the Special Constabulary, contractors, staff employed on a temporary basis and delivery partners staff) of their responsibilities in using all Force e-mail and internet facilities and the procedures to be adopted to ensure that good practice is upheld thereby ensuring the confidentiality, integrity and availability of the Force's computer systems and the data held thereon, and to contribute to the efficient running of these systems and all the associated applications and other systems dependent upon them.

The Force wants to encourage the use of electronic and technological media in the conduct of its business. The Force expects you to access points of contact (e.g. e-mail Inboxes and Broadcast) during each shift, to use these facilities sensibly and act professionally as you would in the normal course of work. For example, when sending e-mail messages, you should use the same safeguards and precautions as you would when sending a fax or letter. Similarly, you should exercise proper judgement as to which Internet sites you visit.

L.1.1 Justification

Providing a direct internet connection substantially increases the chances of importing security risks onto the force network and the main security concerns are:

- The risk of importing malicious or defective software;
- The risk to the force network from external and internal hackers exploiting the connection.
- The risk of sensitive information being released onto the Internet through the actions, accidental or otherwise, of force personnel.
- The risk of sensitive information being disclosed in transit.

In addition the City of London Police has a responsibility to ensure the highest level of public confidence by developing the necessary strategies to prevent corruption, dishonesty, unprofessional and unethical behaviour and to investigate any such incidents that may be brought to attention. In particular, it is the responsibility of the Head of the Professional Standards Unit to create systems to ensure that all information and intelligence is handled, securely stored and disseminated appropriately, and ensure that the City of London Police appropriately apply the legislation governing data protection.

L.1.2 Monitoring

For the purposes of network security, efficiency and maintenance, and compliance with this procedure, the force uses a variety of automated electronic systems to monitor internet and e-mail traffic data[7]. These also provide records to support appropriate incident reporting, response, investigation and system accreditation.

The Force reserves the right to, access, retrieve, review and delete the following without notifying the individual concerned: -

- All e-mail sent, received or in the course of composition.
- Mail boxes and private directories.
- All use of the internet and all other communication techniques deployed by you using the systems; and
- Any third party screen savers, software, materials, etc. on the systems.

The force network and its applications do not provide for the sending, receiving or otherwise storing private, personal, or 'in-confidence' electronic communications. The systems have been designed and should be used for business purposes and for carrying out activities consistent with your responsibilities.

[7] "traffic data" means the data used to facilitate communications **but not** the content of that communication.

L.1.3 Compliance

It is important that you read each section that affects you or your work since you will, forthwith, be deemed to be aware of its contents in the event that there is any breach of Force policy.

This procedure must be followed at all times and it applies to all the Force's computer equipment and facilities, whether or not they are part of the Force network.

Just as with other modes of communication, in all your dealings on the Internet and through the use of e-mail, you are required to observe all legal requirements and the requirements of the APP Code of Ethics, Police Code of Conduct, Corporation Code of Conduct (stated in the Staff Handbook), Force Orders and the Force Information Security Policy.

You will be liable to disciplinary action if you abuse or misuse the systems.

L.2 General Requirements

L.2.1 Mandatory Standards

You will not engage in any activity, which is illegal, offensive or likely to have negative repercussions for the Force. Particularly, you must not access, upload, download, use, retain, distribute or disseminate any images, text, materials or software which:

- Are or might be considered to be indecent or obscene; or
- Are or might be offensive or abusive, in that its content is or can be considered to be a personal attack, rude, sexist, racist, or generally distasteful; or
- Tend to disparage or harass others; or
- Encourage or promote activities which make unproductive use of your time; or
- Encourage or promote activities which would, if conducted, be illegal or unlawful; or

- Involve business activities outside the scope of your responsibilities – for example, unauthorised selling/advertising of goods and services; or
- Might affect or have the potential to affect, the performance of, damage to or overload of the Force systems, network and/or external communications in any way; or
- Might be defamatory or incur liability on the part of the Force, or adversely impact upon the image of the Force.

Any police action or instruction which requires, or may require, supporting evidence of that action must be confirmed in writing and signed by an authorised signatory in accordance with Force Orders.

You are responsible for the security of your password(s) and any action taken under those account details issued to you[8].

L.2.2 Intellectual Property

Broadly speaking, intellectual property refers to copyright material, designs, patents, trademarks, inventions, ideas, know-how and business information. Most images, texts and materials are protected by copyright; others are protected by trademarks.

All intellectual property created in the course of employment belongs to the Force. All computer equipment, software and facilities used by you are also proprietary to the Force, including all documents, materials and e-mails created.

The downloading, possession, distribution or copying of a copyright work is an infringement of copyright unless the person is properly authorised to do so by the copyright owner.

You cannot agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of your line manager/business manager and the Head of Technological Services.

[8] The Password management information can be found in within the Access Control Standard Operating Procedure.

L.2.3 Contractual Processes

All purchases of equipment and services must be conducted in accordance with the Corporation of London Purchasing Rules.

L.2.4 Cryptography

The use of any products for the encryption or scrambling of any e-mail or other document are forbidden, unless authorised by the Head of Professional Standards after submission of a business case via the Force Information Security Manager. If so authorised you must ensure that the force Crypto-custodian is given:

- a complete and up-to-date copy of any private, public, or other decryption key, and
- all other information required for the efficient decryption of the original data.

L.2.5 Anti-Virus Precautions

You must not download any programmes, applications, binary or bitmap files. If such is required in the course of your duties contact the Technology Operations Manager who can arrange for verification of the source and virus checking of the material that is downloaded. If virus infection is suspected do not take any action but inform the Technology Help Desk (ext. 2275) immediately and notify the Force Information Security Manager (ext. 2704).

L.2.6 The Law and Electronic Communications

See Appendix C

L.3 Use of eMail

L.3.1 General

Care should be taken when using e-mail because e-mail messages are perceived to be less formal than paper based communication and there is a tendency to be lax about their content.

All expressions of fact, intention and opinion via e-mail can be held against you and/or the Force in the same way as verbal and written statements. Do not include anything in an e-mail that you cannot or are not prepared to account for. E-mails, both in hard copy and electronic form, are admissible in a court of law.

All members of the Force will be allocated a mailbox in which all mail, including external e-mail can be received. You are allocated an e-mail address for receiving external e-mail; this should only be disclosed, as necessary, in the course of your duties. It should not be used as a contact for commercial purposes i.e. Supermarket shopping, clothes shopping etc.

All email communication must be conducted though the provided force email system. The use of any other email provider, e.g. hotmail/ google mail, is expressly prohibited.

You must not falsify e-mails to make them appear to originate from someone else, nor use anonymous mailing services to conceal your identity when using e-mail services, except for approved purposes (e.g. covert operations).

Never send passwords or any other security codes by e-mail.

Do not send, or forward junk/SPAM e-mail.

Restrict messages to the appropriate recipients and **take care** when addressing e-mails.

Regularly delete messages from your Inbox and Sent Items areas.

The email system must not be used as a records management storage area and emails must be stored within the force network The system will automatically remove any messages that reach 12 months old and information will not be retrievable.

L.3.2 Additional Anti-Virus Precautions

The force employs a range of technical anti-virus measures, but the increasing number and variety of viruses being released means that these measures can never be 100% effective.

Viruses are normally contained in e-mail attachments so if a user is careful in the handling of attachments, the risks of virus infection can be reduced significantly. You are therefore expected to consider the following when opening an e-mail with attachments:

- Is this someone I normally receive attachments from?
- Was this attachment expected?
- Are they asking/tempting me to open it? (Normal business practice tells us that the sender doesn't tell you open the attachment).
- Is there something in the e-mail that doesn't seem right?

NEVER open an attachment that you are **NOT** expecting. If you are unsure contact the Force Information Security Manager immediately.

E-mail does not have to contain an attached file to trigger a virus, some are activated by simply opening the e-mail. You are therefore advised to turn off the **Inbox Preview Pane** in MS Outlook (select **View** in the menu bar then click on **Preview Pane** to remove the preview facility).

Virus warnings will only be distributed by the Information Management Department or the IT Helpdesk. If you receive any virus warnings (many are hoaxes) forward them to either of the above units for verification[9].

[9] Separate arrangements exist for UNIRAS alerts received by the Control Room.

L.3.3 Document Handling

When the content of a document is to be transmitted electronically, the document should be **attached** to an e-mail. The 'cut and paste' facility offered by MS Word should be avoided as it may compromise document security.

Recipients of e-mail are responsible for the security and integrity of any attachments they receive. Attachments should be saved as separate documents and then deleted from e-mail boxes.

When utilising any 'auto forward' facility check the conditions to be applied are secure before activating and ensure that the recipient(s) are appropriate for any mail that will be passed to them. **Auto forwarding to external email addresses is expressly prohibited**. Check with the Force ISO if unsure or for further guidance.

If you receive an e-mail and/or attachment, which contains illegal or offensive material, immediately inform a line manager and the Force Information Security Manager (ext. 2704). Do not delete or forward the e-mail/attachment.

L.3.4 Classification of Documents

E-mail containing information classified up to **RESTRICTED**[10] may be passed freely throughout the Force and Criminal Justice (CJX) networks. **CONFIDENTIAL** information may be passed within the force network if absolutely necessary, suitably password protected and with the permission of the Head of Division/Department (this does not permit the storage/processing of **CONFIDENTIAL** information on the force network).

Information classified at **RESTRICTED,** or higher, must not be transmitted over the Internet, i.e. non pnn, gsi, mod, nhs.net and cjsm addresses.

If your e-mail content is **NOT PROTECTIVELY MARKED** it may still be confidential in nature and you should ensure that the recipient is comfortable

[10] HMG Protective Marking Scheme Standard. All such references will be shown in bold capitals.

with this means of communication, be aware that other persons may have access to the recipients messages[11].

L.3.5 E-Mail and the Force Records Management System

E-mail is an effective method of written communication and is increasingly replacing the use of letters and memoranda. Wherever practical staff should place City-I identifiers (previously registry file reference) on e-mails in just the same way that they would for other forms of documentation. Emails that record organisational decision-making must be saved to the force network alongside the relevant supporting material. **The email system will automatically delete any information over 12 months old, so users are advised to apply sensible housekeeping rules to their email records.**

It is vital that gaps in force policy, knowledge and records do not appear whilst the force operates both manual and electronic administrative systems.

L.3.6 Broadcast

It is intended that the force broadcast facility should be used only for policing purposes and welfare related issues. It will not be considered appropriate for the broadcast to be used for matters of a trivial nature; classified advertising; to pass information to a small identifiable audience when a direct e-mail may be more appropriate; nor for the dissemination of sensitive or classified information. An alternative public folder, Notices, has been made available for non-operational matters to accommodate the demand for other services.

Information Management Services will monitor use of the broadcast in order to maintain standards in line with this procedure and other force policies.

L.3.7 Access to Mailboxes

In addition to the monitoring provisions of this procedure or a formal investigation, other third party access to mail boxes will be subject to permission from the Professional Standards Director upon application through

[11] The conditions of use of many commercial ISP mail services assume ownership of the information stored on them. The use of external e-mail addresses should not be obviously attributable to the force and authorised by the relevant division/department head.

the relevant Head of Division/Department. This permission will only be for operational reasons and because of the absence of the box holder. All such requests and the decisions made will be recorded.

L.3.8 Global Address List and External Addresses

The global address list is a useful tool for the dissemination and reuse of email addresses across the organisation. However, a naming convention **MUST** be followed when recording external recipients in the Global Address List. This will take the format of a prefix "EXT_" before any descriptive information is provided, therefore the email address of "Smith, Gary Gary.Smith@Example.com" will be recorded as "EXT_Smith, Gary Gary.Smith@Example.com". In addition, where an external address is included within a distribution list then this list **MUST** take the format of a prefix "EXT_" so that all users are aware of the external distribution. These steps are necessary to prevent the accidental sending of any information to an external recipient. The ICT Department are responsible for the daily management of the Global Address List and are the responsible owner of this system and its administration.

L.4 Use of the Internet

L.4.1 General

The Internet is provided for business purposes. Users are reminded that when visiting an Internet site the forces identity (IP address) may be logged; therefore any activity engaged in, undertaking given or transaction made might impact upon the force.

When entering an Internet site, always read and comply with the terms and conditions governing its use.

If you arrive unwittingly at a website that contains illegal or offensive material you must disconnect from the site immediately and inform a line supervisor and the Force Information Security Manager (ext. 2704).

Particular care should be exercised when gathering evidence from the Internet to ensure that it has been done in accordance with PACE and other relevant legislation. It must be remembered that prior to any action being taken as the result of information received from the Internet the information must be validated, so far as is possible, to ensure the reliability of the information. Access for **investigative purposes** must be undertaken on a **standalone** Internet enabled machine.

Publication of information onto the Internet must be co-ordinated by the Corporate Communication department. Personal views regarding policing matters should not be published unless previously authorised by the relevant Head of Division/Department.

The following activities are expressly prohibited:

- The introduction of packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
- Seeking to gain access to restricted areas of the network;
- Using Internet based email systems, i.e. Hotmail, googlemail, etc
- Knowingly seeking to access data which you know, or ought to know, to be confidential unless authorised to do so;
- Introducing any form of computer viruses; and
- Carrying out any other hacking activities.

L.5 Personal Use

L.5.1 General

In exceptional circumstances the system and/or the facilities may be used for your own purposes, this use will be within the rules and caveats stated in this standard operating procedure. Any personal communication or Internet interaction must not be excessive in duration, size or content; users should distinguish personal e-mails from business-related e-mails by marking them as NOT PROTECTIVELY MARKED – PERSONAL or PRIVATE - in the subject line.

In addition, you will ensure that your personal use of the system does not:

- take priority over your work responsibilities;
- overload the communications system you are using;
- interfere with the performance of your duties;
- incur unwarranted expense on the Force; and
- have a negative impact upon the Force in anyway.

Personal use of email and Internet systems is not exempt from usage monitoring or auditing.

Personal use does not include onward transmission of written or picture “jokes”, personal photographs, video and audio clips – all of which, if not for business purposes, should not even be on the network.

M Physical and Environmental Security

M.1 Overview

In order to comply with elements of law, HMG and industry best practice, and mandated security frameworks such as the Criminal Justice Community Code of Connection, access to City of London Police's equipment and physical environment as well as information must be protected.

The aim of this policy is to prevent unauthorised access to both physical and electronic information. In summary, the policy requires the following to be protected:

This protection may be as simple as a lock on a filing cabinet or as complex as the security systems in place to protect City of London Police's IT data. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access, loss or other compromise. Information Asset Owners are responsible for assessing the level of protection required.

M.2 Policy Statement

The purpose of this policy is to establish standards in regard to the physical and environmental security of City of London Police's information. All City of London Police employees, partners, contractors and other users with access to City of London Police's equipment and information (electronic and paper records) are responsible for ensuring the safety and security of City of London Police's equipment and the information that they use, store or manipulate.

M.3 Scope of the procedure

This procedure applies to all users of City of London Police's owned, leased or hired facilities and equipment. The policy defines what paper and electronic information belonging to City of London Police should be protected and, offers guidance on how such protection can be achieved. This policy also describes

employee roles and the contribution staff make to the safe and secure use of Police information.

M.4 Secure areas

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage and interference.

M.4.1 Physical security controls

Physical security controls are intended to protect the organisation and its staff, including visitors from violence and protectively marked and other valuable assets from attack by individuals or organisations that are not authorised to have access to them. Such controls often combine some degree of controlled entry through a secure perimeter, with one or more layer of other physical security controls closer to the assets. They should also take account of the security status of individuals who work or visit such areas and meet any requirement for contingency.

The areas of physical security that need to be considered include:

- Document handling - including transfer, accounting, copying and carriage;
- Buildings;
- Rooms, including strong rooms;
- Security containers;
- Locks;
- Entry and Access Control Systems;
- Guards;
- Intruder detection;
- Perimeter security - including the use of CCTV and perimeter intruder detection;
- Destruction of protectively marked waste and other valuables;

- Working on protectively marked assets away from official premises – for example, at home or when travelling and planning for:
- Accommodation moves;
- Conference security;

A balance of physical security controls is needed to meet a system's security requirement. This is likely to be struck between effective perimeter security and protection of the assets involved through, for example, the use of strong rooms and security containers. The type and mix of controls required will depend on the nature of the threats, the cost-effectiveness of the controls, the site and its surrounding environment, sole or shared occupation of the site and if public right of entry is an issue. information asset owners and their contractors are required to ensure that effective arrangements are in place for the appropriate protection of the protectively marked and other valuable assets they hold. Good security can only be achieved with the co-operation of all

M.4.2 Physical security perimeter

The security of the perimeter should be consistent with the value of the assets or services under protection. Secure areas in relation to information security; generally fall into two categories, namely sensitive and secure zones.

Sensitive zones may be defined as areas where the value or confidentiality of the information is high. For example, personnel information, financial management information and Police National Computer terminals.

Secure zones are communication and computer rooms that support business critical activities.

M.4.3 Physical entry controls

The Chief Force Information Security Manager (Director of Information) has overall responsibility for force physical security.

The minimum standards that should be applied are detailed below.

In reception areas, City of London Police staff, to control entrance. Alternatively, other responsible persons or organisations approved by the responsible person.

Entrance to all buildings must be protected by appropriate entry controls. All visitors must register their details at the Front Desk where a Visitors Pass will be issued and entry/departure times from the building of the visitor logged.

Any external staff requiring regular entry to force premises will be issued with an identity card on successful clearance from vetting. No external staff, including the Corporation of London, is to be permitted unaccompanied access to force premises.

Staffs that do not possess swipe cards must validate their identity with a member of the Front Office staff prior to entering a building and be issued with a temporary pass.

Identity cards should be displayed at all times by non- uniformed staff.

Users are to ensure that workstation monitors, printers and any output are not overlooked by unauthorised persons.

Staff passes and Warrant cards will be recovered from staff leavers in accordance with Force Orders and HR policy.

M.4.4 Securing offices, rooms and facilities

Secure or sensitive areas should be subjected to a risk analysis by the relevant information asset owner and appropriate higher levels of protection afforded.

As a minimum the following measures will apply:

- Authorised personnel only.
- Access restricted to necessity basis with visitors or contractors supervised at all times.

- Areas locked and checked out of hours,
- Support equipment (photocopiers, fax, printers, etc.) sited to minimise risk of compromise of sensitive information.
- Prevent photography or other means of recording.

Recommended confidential area measures – Include those recommended above plus entry audit facility, alarm facility, fire control system, regular cleaning by specialist personnel, environmental controls and alarms.

M.4.5 Working in secure areas

Personnel working in secure or sensitive areas must exercise greater vigilance. Any security incidents or weaknesses must be reported immediately to a line manager.

M.4.6 Isolated delivery and loading areas

Delivery and loading areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access or compromise.

M.5 Equipment security

M.5.1 Equipment siting and protection, Power supplies, Cabling security, Equipment maintenance

Any defective or redundant hardware should be disposed of in accordance with the current advice received from the Force Information Security Manager.

Apart from the exchange of specific parts, hardware should not be altered, modified, added or removed without the authorisation of the relevant information asset owner.

No remote diagnostic links are to be installed without the permission of the Information Technology Director and the Force Information Security Manager. Any connections must comply with HMG standards.

Any defective equipment should be suitably isolated from the system before any maintenance work can proceed.

Equipment should be sited or protected to reduce the risks of damage, interference and unauthorised access.

Equipment should be protected from power failure or other electrical anomalies.

Equipment should be adequately maintained and each piece of equipment should have a maintenance record. Maintenance should be carried out in accordance with the manufacturer's instructions. This will ensure continued availability and integrity.

Power and telecommunication cabling should be protected from interception or damage.

Portable IT systems (laptops etc.) used on the force network must not be linked to any other IT system or network without prior approval of the Force Information Security Manager.

M.6 Security of equipment off-premise

M.6.1 General

Information systems equipment may only be removed with the express permission of the relevant information asset owner. No information systems equipment may be used for unauthorised or private purposes. Private equipment may not be used for City of London Police business, unless authorised by the information owner and such use is in accordance with the requirements of the Force Information Security Policy. Thereafter the authorised person will be responsible for ensuring any necessary security controls are implemented and maintained. For example, Force laptops may not be used for personal affairs such as games or home finance. And personal home computers may not be used to perform force tasks, such as the preparation of files, unless authorised. To gain authorisation a member of staff may have to implement physical and technical security requirements at their own expense.

IT equipment may only be removed from the Force local secure environment in accordance with the security guidelines, and all equipment used for such information processing will be subject to regular recall and audit.

N Protective Monitoring

N.1 Aims and Objectives

The City of London Police, by virtue of Section 6, Human Rights Act 1998, is a public authority and is required to act in a manner that is compatible with the rights outlined in the Convention.

The Regulation of Investigatory Powers Act 2000 (RIPA) enables the Secretary of State to make regulations setting out those circumstances where it is lawful to intercept or monitor communications for the purposes of carrying on a business. These regulations apply equally to public authorities.

Various legislation and codes of practice including the Data Protection Act 1998, ISO 27001/2 Information Security Management Systems and ACPO Community Security Policy impose a positive duty on the Force to protect its information assets and provide the assurances that appropriate controls are in place.

The monitoring of staff activity is an established concept which includes the routine supervision of performance and staff behaviour. RIPA extends the principle of supervision to the use by staff of communications equipment provided by the organisation for business purposes.

The procedure applies to City of London Police Officers, Police Staff, Partners, agents and approved persons working for or with the Police

Protective Monitoring is a lawful and ethical tool used to assist the Force in the protection of its staff, information and to assist in the investigation of misconduct or criminal activity. Auditing systems monitor and record all computer based actions conducted using any City of London Police computer equipment.

This procedure defines the monitoring and auditing of staff activity as a means of ensuring all staff comply with Force policy and procedures and with the standards of behavior expected by the City of London Police.

This procedure does not over-ride any existing policies or negate any existing guidance regarding information security, data protection or acceptable use. It is intended that it will supplement such policies but with a specific focus on the protective monitoring of the force computer network and access to the data held within or transported by it.

Main aims and objectives are:

- To ensure the data integrity of the information held by the City of London Police and enhance operational security of criminal investigations. This will be achieved by way of a single force-wide network based facility that will audit computer and peripheral device usage independent of any specific application. The system will ensure that City of London Police complies with the ACPO Community Security Policy (CSP) requirement to carry out “Protective Monitoring”.
- To identify misuse, monitor exceptional usage and support intelligence led investigations. All users of City of London Police LAN accounts must note that the monitoring system will include any personal use staff make of Force equipment, even if undertaken in their own time and with Management agreement. Standard use of all City of London Police systems and information is identified to all users as for ‘Business Use Only’.
- To provide a forensic capability to the auditing process to ensure its evidential credibility.
- To protect the Force by providing the Counter-Corruption Unit (CCU) with the means by which they can effectively seek out those who abuse their position within the force for personal gain or benefit of others.
- To instil within the communities of City of London the confidence that those employed by City of London Police maintain the highest levels of honesty and integrity by enforcing the relevant Codes of Conduct in relation to unethical behaviour or gross misconduct.
- To protect the information and intelligence assets of the Force from malicious or accidental disclosure.

N.2 Definitions

Protective Monitoring – The term given to an auditing capability that is network based as opposed to being application specific.

Application – Refers to the software installed on force computers/servers, virtual or otherwise, that will facilitate the logging of actions conducted by the user logged on to a specific terminal or access point.

Console – The administrative and querying interface of the application used to interrogate and manage the system.

Intercept – The "live" monitoring of communications which may involve recording of any activity witnessed.

Monitor – The review of "historic" data recorded and stored within the auditing database.

Communications Equipment – Any equipment that facilitates the creation, transmission or receipt of data provided by the Force and intended for the business use of the City of London Police.

N.3 Administration

The Protective Monitoring data will be stored and controlled in accordance with the controls commensurate with a RESTRICTED system.

The auditing systems will be administered by nominated MV/SC vetted staff.

Routine reviews of the audit data will be conducted to ensure compliance with relevant legislation.

N.4 Access

Data stored within the Protective Monitoring system will only be accessible to suitably trained members of CCU; access to pre-defined Management Information reports will be available to other Professional Standards staff members as appropriate.

Requests for quantitative/system data must be submitted to the DCI - CCU and each case will be considered on its own merits. Such requests must be made with the authorisation of an officer of the rank of Chief Inspector or above or police staff equivalent.

No personal data will be disseminated outside the department without the explicit instructions of the Department head.

N.5 Security

Data stored within the database is afforded the physical and protective security measures required for RESTRICTED material.

Passwords entered by force network users are not exposed to audit and remain known only to the user.

All system users and administrators are audited including those with access to the software terminal console.

N.6 Publication / System Warnings

A suitably worded logon script is shown at the point each individual user logs onto a force computer. The text explains in plain language that access to the force network is for authorised users only and is monitored. Users are advised that they should have no expectation of privacy if they choose to use the Force computers for personal use. They are also reminded that personal use must be only be conducted following recorded agreement with Line Management.

Attempts to disable/prevent installation or otherwise deliberately interfere with the functionality of auditing software will be considered a misconduct matter and investigated appropriately. Interference with the system may also constitute an offence under the Computer Misuse Act 1990 and would be treated as a criminal matter.

Information generated by the Protective Monitoring audit systems may be used as grounds for further enquiries and form the basis for further investigation.

The results of audit log interrogation may be used as evidence in misconduct and criminal proceedings.

N.7 Data Protection

The Data Protection Act 1998 provides for the regulation of the processing of information relating to individuals, including the obtaining, holding, use and disclosure of such information.

Any information relating to an individual or their actions generated by the audit system will be subject to relevant legislation and protected accordingly.

It is the responsibility of the system owner to ensure that all aspects of the Data Protection Act are complied with.

The requirements for data review, retention and disposal will be applied in accordance with the provisions of the Data Protection Act 1998 and the Management of Police Information (MoPI) Codes of Practice 2010.

O Remote Access to Force Systems

O.1 Overview

The purpose of this procedure is to detail the standards for connecting to the CoLP network from devices that are outside the network perimeter. These standards are designed to minimise the potential exposure of CoLP from damage that may result from unauthorised access to their information assets, or computing resources. Potential damages include the loss of confidentiality, integrity or availability of force confidential data or intellectual property, damage to public image, or damage to CoLP internal systems.

CoLP will comply with CESG Infosec Memo 35 – Remote Access to Public Sector IT Systems. This Remote Access procedure is intended to provide specific information relating to CoLP use of remote access.

O.2 Objectives

The objectives of this SOP are to:

- Protect the systems and infrastructure of the CoLP network, and the information held thereon from damage, degradation or unauthorised access;
- Protect CoLP information from risks that could arise from remote access;
- Meet the requirements of all applicable legislation.

O.2.1 Security Principles

The connection by remote access of any device, by any individual, is subject to the same policies, standards and controls that are applied for access within the CoLP network.

- Before remote access is granted, it must be confirmed that there is a valid operational or business reason for that access.
- Remote access facilities will only be available for the purpose and duration for which they are granted. In the event that the requirement for any individual changes, the change will be subject to the approval process.

- Access may only be permitted from approved known devices, in the possession of known individuals who have been vetted to a level that is appropriate for the sensitivity of the information to which they will have access.
- Strong authentication will be used to avoid the risk of unauthorised remote access. This authentication will comply with the current Unified Police Secure Architecture.
- Encryption will be used to protect information in transit across communications links.
- All accesses will be recorded and proactively monitored, and the activities performed will be logged. The logs will be reviewed regularly, and any suspicious activity will be investigated.
- All devices that are approved for remote connection to the CoLP network will be free of unauthorised code, such as viruses, and will be configured to ensure that they remain so.

O.3 Scope of this Procedure

This policy applies to all users of City of London Police facilities and equipment including staff and any third party suppliers and contractors. All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

O.4 Responsibilities

O.4.1 Users of remote access facilities

Employees of CoLP or its agents must ensure that their remote access connection is given the same consideration as their on-site connection to the network.

Users will not connect any system to the CoLP network without prior approval of its configuration by the CoLP Technology Unit.

Users will ensure that all systems that connect to the CoLP network use the most up-to-date version of anti-virus software and virus definitions.

Employees of third parties, including service organisations must comply with the CoLP Security Policies, and with the Third Party Connection Agreement (Appendix E).

Employees of other organizations, forces or agencies are expected to comply with the Force Information Security Policy and be explicitly identified within relevant procedural document and/or contract.

Users must not reconfigure systems that have been set up or approved by the CoLP Technology Unit without direct instructions from the Technology Unit.

Users must not divulge their password to anyone and will take care to ensure that others do not overlook the access process. If they suspect that their password is known to anyone else, they will change it immediately, and if they suspect that someone else has used their password, they will change it immediately and report it using the CoLP Incident Reporting and Management Procedure.

Users will not share any material or token for authenticating remote access.

Users will only use the connection to perform the activities for which the access was approved.

Printouts may only be produced remotely by exception and requires a detailed business case, approved by the SIRO. This is due to the normal lack of assurance of remote locations where the material is to be produced.

Users must ensure that systems in non-secure areas are not left unattended while logged on, and are logged off and disconnected from the CoLP network at the end of the session.

O.4.2 Managers

Managers are responsible for requesting remote access for their users. This involves the following activities:

- Define the business case.

- Ensure that the individual has been appropriately vetted for the access required.
- Where applicable, ensure that a Third Party Access Agreement is in place and all appropriate checks are made prior to requesting approval from the Information Management Board.
- Identify the specific activities required for remote access – these may not be as comprehensive as those required within the network, and special consideration should be given to the sensitivity of the information to be accessed, the location from which it will be accessed and the Impact Level.
- Arrange, and obtain approval for loan equipment if required.
- Periodically (at least 6 monthly) review the requirements for remote access.
- Advise the Technology Unit when the requirement for remote access no longer exists.
- Ensure that the individuals are fully aware of their responsibilities.

O.4.3 Technology Unit

The technology unit are responsible for ensuring compliance with technical aspects of this policy by:

- Securely configuring loan equipment in accordance with the document entitled “Security Conditions to be met before working outside of CoLP premises with a CoLP computer system” before and after use.
- Issuing tokens and administering the RSA Secure-ID token system.
- Reporting security incidents, whether actual, suspected or potential to the Force Information Security Manager.
- Keeping asset records for loan equipment.
- Reviewing access and event logs.

O.4.4 Information Management

Information Management are responsible for providing assurance to the SIRO in respect of appropriate security measures and will be responsible for:

- Ensuring that remote access to CoLP I.T systems complies with CESG Memo 35 and HMG Infosec Standard No 4.
- Providing advice to remote access users on the security requirements of their own systems.
- Periodically (at least 6 monthly) review access logs and inspect all connections to the RESTRICTED Network.
- Overseeing and assisting with the risk assessment on users, communications methods and locations based upon the Impact Level of the information to be accessed.

O.5 Monitoring and Inspection

O.5.1 Monitoring

All external connections to the CoLP network will be logged, and the user, location and times of access recorded. All access to CoLP systems will also be logged.

These logs will be reviewed. If any unauthorised access is identified the CoLP will remove access from the individual(s) concerned.

O.5.2 Inspection

The CoLP will inspect the security arrangements of those with external access on a regular basis, and reserves the right to conduct such inspections without warning. The purpose of any inspection will be to ensure that the requirements of this SOP are being met.

O.6 Security of Third Party Access

O.6.1 General

Access by third parties poses a risk to City of London Police information systems. Before any connection is undertaken the information asset owner

will conduct an analysis of the risks. Appropriate security controls will be adopted. Any connection must be subject to a contract, which must specify the security requirements. No connection may be made without the express permission of the Information Technology Director and the Chief Information Security Officer.

O.6.2 Outsourcing

Outsourcing the management or control of information systems poses a risk to the City of London Police. Before any outsourcing is undertaken the information asset owner will conduct a risk analysis. Any risk must be managed to ensure the confidentiality, integrity and availability of information. Any outsourcing must be subject to a contract, which must specify the security requirements. No outsourcing may be made without the express permission of the Information Management Board.

For information asset owners managing protectively marked assets, security is the central issue in any procurement or outsourcing project. It is recognised that, at the outset, the detail of the security requirement may not be known. However, strategic requirements for CONFIDENTIALITY, INTEGRITY and AVAILABILITY should be specified in the invitation to tender and the award of contract must be subject to assurance that the contractor is capable of meeting detailed security requirements.

O.6.3 Legal Compliance

General

Arrangements involving third party access force IT facilities, information, or personal data should be based upon a formal contract containing, or referring to, all of the necessary security conditions to ensure compliance with this procedure. This contract should be in place before the access is provided.

Data Protection Act

The Data Protection Act 1998 requires that where the processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle:

- choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
- take reasonable steps to ensure compliance with those measures.

Where the processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless:

- the processing is carried out under a contract:
- Which is made and evidenced in writing; and
- under which the data processor is to act only on instructions from the data controller.
- the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

The most common situations involving the handling of such assets by individuals and organisations outside the force are:

- Contractors working on force premises
- Contractors working on their own premises
- Consultants

P Business Continuity

P.1 Overview

The City of London Police has a legal responsibility under the Civil Contingencies Act 2004 to deliver their core functions to the community as a whole.

Information Technology services are paramount in supporting the provision of key departments and sections. It is vital that information asset owners build resilience into the provision of their system(s) to support the force.

P.1.1 Aspects of business continuity management process

A managed process should be developed and maintained, including identifying sufficient financial, organizational, technical and environmental resources for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.

Information asset owners must ensure that contingency plans are in place to cover the continuity of essential business operations and services. These include but are not limited to IT services. Plans should be exercised regularly.

Contingency Planning involves identifying the most likely failures and defining effective plans of response should those failures occur. Where appropriate, plans should address not just long-term recovery from failure, but also interim measures to assure a minimum level of service while recovery is in progress.

Contingency Plans should cover such issues as (but not limited to):

- system failure
- network and telecommunications failure
- effects of fire and flood
- effects of terrorist attack, and
- recovery procedures.

P.1.2 Business continuity management process

Plans covering procedures to follow in the event of a contingency are laid out in the Force IT Contingency Plan. The plan provides an alternative means of continuing processing in the event of any damage to or failure of the force network. Owners of other systems should adopt similar procedures.

A formal method of change control is needed to ensure that the implications of change are identified and disseminated prior to updating and redistribution of the Plan.

P.1.3 Business continuity and impact analysis

Information management continuity plans will be based on an appropriate risk analysis and shall be consistent with the force's overall approach to business continuity, as defined within the Business Continuity Policy.

P.1.4 Writing and implementing continuity plans

The relevant information asset owner will develop plans to restore business operations following interruption to, or failure of, critical business processes. Consideration must be given to all aspects of the restoration process not merely the IT services.

P.1.5 Business continuity planning framework

Emergency procedures to address major incidents or interruptions to Force core functions and critical activities are contained within the Force Business Continuity and Emergency Plans and associated Force IT contingency plan. City of London Police information asset owners must develop procedures consistent with established frameworks. The plans shall also identify priorities for regular testing and maintenance. Responsibilities will be clearly identified and agreed.

P.1.6 Testing, maintaining and re-assessing business continuity plans

The relevant information asset owner is responsible for identifying and applying changes to the plan. The need for individual changes should be reviewed at least annually. This process should be reinforced by a brief annual review of the complete plan.

Q Human Resources Requirements for Information Security

Q.1 Overview

City of London Police holds large amounts of personal and confidential information. It has a variety of statutory, regulatory and internal obligations to process this information in a way that assures its confidentiality, quality and availability at all times. Security cannot be achieved by technical means alone. It must be supported by effective processes and people. This procedure addresses security issues related to people.

Q.2 Procedure Statement

City of London Police understands that to reduce the risk of loss, theft, fraud, inappropriate or criminal use of its information systems, anyone that is given access to Police information systems must be fully identified to national standards, and be suitable for their roles. They must fully understand their responsibilities for ensuring the security of the information, and that they must only have access to the information they need, and that this access must be removed as soon as it is no longer required.

Access to Police information systems will not be permitted until the requirements of this policy have been met.

Q.3 Scope of the Procedure

This procedure applies to any person that requires access to City of London Police information systems of any type or format (paper or electronic).

The policy applies to all Police employees through their contract of employment and its enforcement is the responsibility of HR and Departmental managers.

Where access is to be granted to any third party (eg temporary staff, contractors, service providers, voluntary agencies, partners etc) compliance with this procedure must be ensured. Responsibility lies with the City of

London Police sponsor that initiates this third party access, in co-ordination with HR.

This procedure addresses 3 key stages of a user's access:

1. **Joiners**: Prior to granting access
   National ACPO identification and vetting checks must be made to ensure that the individual is suitable for access to Police and other criminal justice information systems. The manager is responsible for co-ordinating system access requirements with HR, based on the user's job role.
2. **Movers**: Period during access

   Users must be trained and equipped to use systems securely and their access must be regularly reviewed to ensure that it remains appropriate. The current manager is responsible for co-ordinating system access with HR, based on the user's job role.
3. **Leavers**: Termination of access

   Where the user's requirement for access ends and needs to be removed in a controlled manner.

This procedure also addresses third party access to City of London Police information systems (eg temporary staff, contractors, service providers, Local Authorities, Quangos, voluntary agencies and other Criminal Justice partners).

R Secure Disposal of Assets

R.1 Purpose

The purpose of this procedure is to establish and define standards, methods, and restrictions for the disposal of CoLP IT equipment in a legal, cost-effective manner. City of London Police's obsolete IT assets resources (i.e. desktop computers, laptops, notebooks, printers and servers) must be discarded according to legal requirements and environmental regulations. Therefore, all disposal procedures for retired IT assets (legacy) must adhere to this procedure

R.2 Scope

This procedure applies to the proper disposal of City of London Police IT hardware, including PCs, laptops, notebooks, printers and servers. City of London Police obsolete machines (legacy), and any equipment beyond reasonable repair or reuse are covered by this procedure. All COLP departments are included in this procedure. Leased equipment must also be cleansed before being returned to the leaser.

R.3 Definitions

- "Non-leased" refers to any and all IT assets that are the sole property of City of London Police
- CoLP Owned; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or partner company.
- "Disposal" refers to the removing of the asset from operating use with the intent of retiring the asset according to the surplus property disposal policy.
- "Obsolete" refers to any and all equipment that no longer meets requisite functionality.
- "Surplus" refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.

- “Beyond reasonable repair” refers to any and all equipment whose condition requires fixing or refurbishing if the cost is equal to or more than total replacement.

R.4 Secure purchase, maintenance, disposal or re-use of equipment

This procedure describes the high level guidance for when information system equipment containing City of London Police information is being disposed of, reallocated within the City of London Police, or removed from a City of London Police site for maintenance or repair. Specific instructions can be obtained from the Force Information Security Manager or Information Technology Department.

When information system equipment becomes surplus to requirement, care must be taken to ensure that its disposal does not expose any City of London Police data that it has processed or stored to an unacceptable risk of compromise. Of primary concern are data bearing components of the equipment, e.g. disks (fixed and removable).

Disposal of equipment by reallocation or sale requires deletion of sensitive material. If the information is actually held on fixed disks, these components must either be removed or be subjected to an approved process whereby the data resident on these devices is obliterated.

R.4.1 Software

Most software, be it end-user, package or system software, is widely available but if not obtained through the normal procurement channels it may be illegal and unsupported. The Force Information Security Manager will provide details of suitable software for the removal of data from force systems.

Software acquired or used illegally renders both the force and individuals open to criminal charges. Software from an unaccredited source, such as a bulletin board or the Internet, may be illegal and is more likely to be of poor quality or malicious (e.g. it may include a virus, covert channel or Trojan

code). Because end-user software is easily acquired and relatively inexpensive, it is more likely to be chosen without proper consideration of its fitness for purpose or its future support and maintenance.

The disposal of software, once it has ceased to be of operational use, may well just involve straight deletion. However in some cases there may be additional contractual obligations to be fulfilled, raising the possibility of a supplier gaining access to proprietary information, either from data originally needed for support purposes or from any returned or reclaimed software. Also the support by a supplier may be reduced during the notice period and external links (for diagnostic purposes) being left connected to the supplier.

Most software cannot be re-sold, under the terms of its licence. Therefore care must be taken to ensure that executable code is not left on any device that is disposed of from the Force.

Consideration also needs to be given to any data that is to be kept. These may need to be converted to another format before they can be used with any new or replacement software, or it may be necessary to retain the software itself until there is no further business need to access the data.

R.4.2 Hardware

The main risks when acquiring hardware are that the equipment may not be properly installed and maintained, may not be sufficiently powerful and reliable for the task and viruses can also be introduced with new hardware. The more critical the system and the more confidential the data stored on the hardware, the greater the risk.

Hardware (e.g. disk drives and memory modules) and consumables (e.g. diskettes and CD ROM's) are discarded because they are damaged, cannot be reused, or have become redundant. With the disposal of hardware and consumables, other than the danger of inadvertent reuse of damaged equipment, the main risk lies with the information and data, which may have been stored on these media. With the appropriate technology most media, even when damaged, can be read.

Equipment needs to be correctly maintained to ensure its continued availability and integrity. The Force, via the City of London Corporation, has a comprehensive maintenance agreement, and insurance for all hardware recorded in the Force asset register. Hardware purchased in accordance with this order will be covered by these existing arrangements.

All hardware must be disposed of in accordance with the Law and Corporate procedures.

All purchasing, maintenance and disposal of IT software, hardware and removable media used for the processing of force data, will be in accordance with this procedure. Any current contractual agreements for such services, which are contrary to the requirements of this procedure, may be continued until the expiry of such, but they must be registered with the Information Technology department. Thereafter this procedure must be complied with.

R.5 Procedure

There are two scenarios that must be considered for disposal.

R.5.1 CoLP owned asset disposal

The current method for the disposal of assets is to physically destroy the device via an IS5 out sourced provider. This is a zero cost solution managed by the Security Team within Information Management Services.

In every instance the Data Cleansing Form (Appendix D) must be completed.

For each computer to be taken out of service, the hard disk drive component will be removed by a qualified IT technician and then transferred to the Security Team within Information Management Services who manage the onward disposal with an IS5 approved company**.** The computer chassis will then be disposed of via the Corporation of London equipment disposal provider, at this time Maxi-tech

R.5.2 Leased asset disposal

Any equipment that is leased remains the property of the lease company and is not therefore subject to physical disposal, unless explicitly agreed with the lease company.

Before returning any leased equipment capable of holding data all of the data stored must be removed from storage area.

The IT department is responsible for sourcing appropriate technical software to cleanse devices to the necessary IS5 standard.

The cleansing technician (IT staff member) is responsible for ensuring any CoLP data, on a device to be returned is properly backed-up and that it is so noted on the Data Cleansing Audit Form, found in **Appendix D**.

Upon completion of the cleaning and sanitizing, the IT technician will complete and sign the Data Cleansing Audit Form, see Appendix D, and submit it to the Force Information Security Manager for future audit purposes. The device can then be returned to the owning company.

S Security Standards for Acquisition, Development and Maintenance of Information Systems

S.1 Security requirements of systems

S.1.1 General

All security requirements should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.

S.1.2 Security requirements analysis and specification

A risk analysis should be carried out to determine the security threats and vulnerabilities of any new systems, or enhancements to an existing system. All systems processing protectively marked information must undergo a technical risk assessment to HMG Infosec 1 Standard. The Information Security Officer can provide the necessary guidance on this standard. Risk assessment is to be commensurate with the force approach to risk assessment.

Any business requirement must specify the security controls required to safeguard the confidentiality, integrity and availability of the information contained within the system.

To achieve this, consideration should be given to access controls, privileges, audit and accounting controls, disaster recovery and statutory requirements.

Data protection standards must be maintained.

Security measures must take into account the physical, operational and technical operating environment.

S.2 Security in application systems

S.2.1 General

Relevant system owners shall validate data input into application systems to ensure that it is correct and appropriate.

Relevant system owners will issue instructions to specify the detailed execution of each task. These instructions will include procedure for correct data handling and entry, error handling, help facilities, handling and secure disposal of output, restart and recovery, correct start-up and close down, back-up, hand-over, security of system documentation, and keeping of logs. Relevant system owners must establish procedures to respond to validation errors.

These procedures must be reviewed annually.

Users must enter and handle data accurately, appropriately and correctly. Failure to do so may lead to disciplinary action.

S.2.2 Input data validation

Data input to applications should be validated to ensure that this data is correct and appropriate.

The following should be checked to detect errors:

- Out of range values.
- Invalid characters in data fields.
- Missing or incomplete data.
- Exceeding upper or lower data volume limits.
- Unauthorised or inconsistent control data.

These checks should be documented and available for inspection.

Automatic examination and validation of input data can be considered, where applicable, to reduce the risk of errors and to prevent standard attacks including buffer overflow and code injection.

S.2.3 Control of internal processing

Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. These checks may be manual or automated. These checks should be documented and available for inspection.

S.2.4 Message authentication

Consideration should be given to message authentication where there is a security requirement to protect the integrity of the message content.

S.2.5 Output data validation

Relevant system owners should conduct validation checks to ensure that data output from stored information is correct. These checks should be documented and available for inspection.

S.3 Cryptographic Controls

S.3.1 Policy on the use of cryptographic controls

A risk analysis should be carried out to determine if encryption is appropriate. The subsequent risk assessment should identify the level of protection required.

S.3.2 Encryption

Relevant system owners will ensure that critical or sensitive information is protected by encryption during transmission or storage. Appropriate, encryption of information can reduce its attractiveness if the attacker is unable to break the encryption. On the other hand, encrypting information can highlight the fact that it is important thus making it more attractive. It is

therefore vital to use the appropriate grade of encryption where it is used at all.

Many forms of encryption involve the setting-up of encryption devices ('crypto equipment') with keying material - paper tape, swipe cards etc. These consumables are collectively referred to as 'crypto material'. Just like physical keys, crypto material needs to be kept under close control. For detailed guidance on the handling and operation of crypto material contact the Force Crypto-Custodian or Force Information Security Officer.

The Information Technology Director, Force Crypto-Custodian and the Force Information Security Officer must approve all cryptosystems before being used for protection of protectively marked information.

Any proposed modification to crypto equipment must be approved through the Force Crypto-Custodian. Changes to commercial equipment will require re-evaluation and re-certification.

S.3.3 Appropriate grades of encryption

The grade of encryption used must assure adequate resistance to attacks. The highest grade of cryptographic protection is designed to resist the severest attacks for many years. Lower grades of encryption protect against lesser attacks for shorter periods.

Approved cryptography within the UK is divided into three grades known since 1996 as High, Enhanced and Baseline Grade.

S.3.4 Digital signatures

A digital signature is a technique that creates a unique and unforgettable identifier for the sender of a message. The digital signature can be checked by the recipient to verify authenticity, a guarantee of the INTEGRITY of the signed message and provides for non-repudiation. Such a signature is only open to forgery if the private key becomes compromised. Within a public key architecture, certificates are used to verify that public keys belong to named

individuals and offer a safeguard against the use of false keys for masquerading purposes.

Consideration should be given to the application of digital signatures to protect the authenticity and integrity of electronic information.

S.3.5 Non-repudiation services

Non-repudiation is a process, which offers evidence that a message or transaction originated by an individual or entity was in fact originated by that individual or entity, or that a recipient of a message in fact received it. It thus frustrates attempts by originators or recipients to deny their involvement. This is particularly important in electronic commerce and any electronic transactions creating legal obligations, for example, contracts.

S.3.6 Authentication

Authentication is a process, which verifies the claimed identity of an originator, recipient or other entity. For example, it can be used to provide assurance that an order or other message transmitted electronically is genuine, or as an aspect of access control to sensitive data. Public Key Cryptography techniques, which provide security features without needing a secure distribution network for large user communities, are good illustrations of the value of authentication. Any user can encrypt using a public key, but only the holder of a private key can decrypt, and vice versa. This sort of authentication system depends on the owners of private keys being the only individuals who have access to their private keys, and mechanisms are often incorporated to verify the authenticity of the various keys that match them to the individuals.

S.3.7 Key certification

Under a public key architecture, it is necessary for the public key and its owner's identity to be encapsulated in a certificate, which is digitally signed by an approved certification authority. The certification authority guarantees the correctness of the information. Secure e-mail and Secure Electronic

Transaction (SET) protocols are examples of the sorts of applications which public key certification can underpin.

S.3.8 Time stamping

Time stamping is a means of allowing users to determine exactly when a document was last modified or created; in effect, a parallel service to authorship guarantees, that have been secured via use of digital signatures.

A digital signature mechanism can be used to provide a means of authenticating the originator of the data.

HMG recommends the use of the Digital Signature Algorithm (DSA).

The use of DSA will only provide assurance to the user if appropriate access controls have been applied to the system(s) they reside on.

The establishment of a non-repudiation mechanism must be the subject of an agreement between the data originator and recipient.

On an internal system where encryption is not required for CONFIDENTIALITY, but privacy is an issue, approved baseline grade cryptography may be used for data separation. The use of non-approved commercial software is not recommended for data separation, as it does not provide any level of assurance.

Consideration should be given to the use of non-repudiation services to resolve disputes about the occurrence or non-occurrence of events or actions.

S.3.9 Protection of crypto material (Key management)

Crypto Key material, may itself, be unencrypted or may itself be protected by encryption. The unencrypted form is obviously more vulnerable. The basic principle governing the protective marking of unencrypted keying material is that it must be given a marking equivalent to the information it is to protect. When filled or keyed, crypto equipment must be handled in accordance with the greater of its own protective marking or the protective marking of the keying material it contains.

Crypto material is to be secured according to its protective marking and in a way that allows access only by appropriately vetted and crypto authorised personnel. An additional marking - CRYPTO - indicates the need to limit access and apply extra controls.

Keying material for systems using Public Key Cryptography (PKC) techniques, such as BRENT, may not have a protective marking, but should be handled as valuable and accountable items.

Crypto equipment must be protected from unauthorised access to prevent loss and any possibility of tampering that might render the system inoperable or insecure. Access to operational crypto-equipment, and keyed equipment in particular, must be limited to employees:

Cleared to the level of the protective marking of the keying material in use and with an operational need to be in the vicinity of the equipment.

S.3.10 Disposal and destruction of cryptoequipment

CESG (Communications-Electronics Security Group, the Information Security arm of the Government Communications Headquarters) are the authority for the disposal and destruction of cryptoequipment.

S.4 Security of system files

Relevant system owners will ensure that IT projects and support activities are conducted in a secure manner.

S.4.1 Control of operational software

Relevant system owners will exercise strict control over the implementation of software on operational systems. Updates to operational software will be documented. Previous versions will be retained as a fallback.

S.4.2 Protection of system test data

Relevant system owners will protect and control test data in the same manner as operational data. Access must be restricted to persons who need the data to perform their function. Records of access will be maintained. Where possible test data should be de-personalised. The provisions of the Data Protection Act must be adhered to with regard to personal data on a test system. An audit trail must be maintained to monitor the use of live data on any test system. Live data on a test system must be destroyed when no longer required. Great care must be exercised to ensure that operational and test data are kept separate.

S.4.3 Access control to program source library

Relevant system owners will exercise strict control over access to program source libraries. All access will be authorised and documented.

S.5 Security in development and support processes

S.5.1 General

Relevant system owners will maintain the security of application system software and information.

Relevant system owners will ensure that the implementation of changes is strictly controlled. Formal change control procedures must be adopted to minimise the corruption of information systems. These procedures must be fully documented and include authorisation procedures, a review of the security implications, implementation of appropriate additional controls and audit logging of all actions taken to implement changes to applications.

S.5.2 Technical review of operating system changes

When change occurs relevant system owners must ensure that applications are reviewed and tested for security impacts. Testing and review will ensure that there is no way of bypassing security functions or provide means of obtaining unauthorised access.

S.5.3 Restriction on changes to software packages

Only software that is entered on the Approved Software Register, managed by the IT department, will be used. The installation of unauthorised software is prohibited. Software must not be modified without the consent of the owner of the software. Before any changes are made to software the risk to security must be assessed.

S.5.4 Covert channel and Trojan code

Covert channels or Trojan code (unauthorised functions allowing unauthorised access) are a risk to information security. All software shall be checked for such threats, prior to installation.

Prevention of unauthorised network access, as well as policies and procedures to discourage misuse of information services by personnel, will help to protect against covert channels.

S.5.5 Outsourced software development

Any external development work shall be subject of a risk analysis and appropriate security controls adopted to protect the confidentiality, integrity and availability of Force information.

S.6 Technical Vulnerability Management

S.6.1 Control of technical vulnerabilities

Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

A current and complete inventory of assets is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what

systems) and the person(s) within the organization responsible for the software.

Appropriate, timely action should be taken in response to the identification of potential technical vulnerabilities.

An effective management process for technical vulnerabilities should consider:

- The organisation should define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required;
- Information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology (based on a asset inventory list); these information resources should be updated based on changes in the inventory, or when other new or useful resources are founded;
- A timeline should be defined to react to notifications of potentially relevant technical vulnerabilities;
- Once a potential vulnerability has been identified, the organisation should identify the associated risks and the actions to be taken; such action could involve the patching of vulnerable systems and/or applying other controls;
- Depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management or by following information security incident response procedures;
- If a patch is available, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch);
- Patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as:
- turning off services or capabilities related to the vulnerability

- adapting or adding access controls, e.g. firewalls, at network borders;
- increased monitoring to detect or prevent actual attacks;
- raising awareness of the vulnerability;
- an audit log should be kept for all procedures undertaken;
- the technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;
- systems at high risk should be addressed first.

Technical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures.

~ APPENDICES ~

A The Secure Use of Passwords

Introduction

1. Proper access control is an essential part of computer security, and most other aspects of computer security depend on it. Password systems are commonly the sole means of controlling access to computer systems. It is important to realise that once the password system is bypassed, the rest of the system is potentially open to exploitation. Users should adequately design, implement and maintain their passwords in support of overall access control in order to safeguard the security of the entire system.

2. Computer systems often use passwords as a means of controlling access to both data and functions. Particularly with larger systems, and certainly within the City of London Police, entry will invariably be controlled by associating user identifications with specific functions. Thus systems are programmed to grant certain rights to particular authorised users - these are known as user rights. That user may be allowed to view all the records in a data base, or be limited to seeing only a subset of the records. He or she may or may not be allowed to create new records, to amend some or all of the information in a record, or to delete records. The user identification may be added to a computer held transaction log so that subsequent audits can discover which user was responsible for any particular transaction carried out.

3. Usually at least one individual, the Departmental Systems Manager, will be allowed to assign user rights to all, or any individual and will be responsible for password management. It is generally best for individuals using the system to have their own password.

4. The password is used to safeguard these rights. Once a system recognises a user identification, (entered as part of the log-on procedure), it will ask for a password. It will then compare this with a table of approved passwords and, if a match is achieved, will grant the specified access rights. Invariably these will remain in force until such time as the terminal is switched off. System

security will be endangered if a user leaves a terminal logged on and unattended.

5. The purpose of this Order is to provide guidance to assist users to prevent passwords being compromised. Passwords must always be kept secret if they are to achieve their purpose. In some cases unauthorised users could exploit the system to the extent of destroying the software and any data it holds.

The Need for Password Security:

6. Passwords are an effective IT security countermeasure only if they can be kept secret. A major problem is that passwords can be passed to, and used by, others without the knowledge of the original owner. It may not be apparent that this has happened and a password so obtained may be used for some considerable period without detection.

7. Unless staff appreciate the need for IT security, they are unlikely to take sufficient precautions to protect the integrity of their passwords. The need to remember and enter passwords detracts from the ease of use of a system, and it is all too common for users to compromise security in their attempts to simplify the use of passwords. All new users should therefore be briefed on the importance of passwords and instructed in the manner in which they are to be used and protected.

8. Some of the ways in which passwords can be vulnerable are set out in the following paragraphs. Countermeasures for reducing or negating these vulnerabilities are also described. The degree to which these measures are implemented is always dependent on the sensitivity of the data and the requirement for confidentiality, integrity and availability. Passwords should always be treated as though classified at the level of the most sensitive data held on the system to which they allow access.

9. Passwords should not be confused with user identifications, (see para. 2), which specify areas and functions accessible to a particular user. The

password is the way in which the system verifies that a particular user is who they claim to be.

Sharing:

10. For the most effective security, staff should have individual passwords and should never reveal them to anyone.(but see para. 11). The simplest form of compromising a password is to tell others what it is. No one has the right to know another's password; not friends, colleagues or line managers. There may be various temptations to share passwords with others depending on working conditions, however a shared password is not good security.

Finding:

11. Obvious though it may seem, and with one exception, do not write passwords down anywhere. The exception is that the password may be written on a slip of paper and placed inside a sealed envelope, classified to the highest level of the data held on the system and protected to that level. The envelope should then be placed in the custody of the departmental officer nominated. Access may then be allowed in exceptional circumstances, e.g. extended sick leave. This course of action should always be adopted for pass worded standalone personal computers.

12. The simplest way in which a password may be revealed to unauthorised persons occurs when it is written down and left in the vicinity of a terminal.

Watching:

13. Another way in which an unauthorised user may "discover" a password is to watch closely while an authorised user logs-on. Whilst it is true that passwords are not displayed on screen as they are entered at the keyboard, it is fairly easy to watch the keys being pressed by a user, if necessary over a number of days, as he or she logs into the system. The shorter the password the easier it is!

14. While it may appear antisocial to ask people to avert their eyes whilst a password is being entered, the only effective countermeasure is to ensure that password entry is never viewed by anyone else.

Guessing:

15. Given a free choice most users will opt for passwords that they find particularly easy to remember. One of the reasons for this is that users do not feel obliged to write down their password in case they forget it. All too often, however, the password chosen has strong associations with either the system or the background of the user and may be guessed by potential intruders.

16. It is a well-documented fact that many users favour passwords that mean something to them personally, e.g. their own name, the name of someone close to them, the name of their house, the name of a pet, a favourite football team or a favourite food. A strong temptation when several people share an application is to also share a password, which may be the application name, e.g. PAYROLL. Potential intruders, particularly those who work in the same area and perhaps know some of the users well often find such passwords easy to guess.

17. Users must, therefore, try to devise passwords that are unique to them and are unlikely to appear on an intruder's test list. Some suggested means of achieving this are given in the next section. Unguessable passwords will never consist of a single dictionary word or name. They will always consist of at least 6 characters, at least one of which will be something other than one of the 26 letters of the alphabet.

18. Unauthorised users may compile a list of likely and commonly used passwords that they will then test against the system until they find a successful match. Such a list is likely to include words like 'USER', 'FRED', 'BATMAN', 'SPURS', 'QWERTY', 'X', 'GUEST', 'BOSS' and 'PASSWORD'.

Secure Passwords:

19. A secure password is one that is made up of at least 6 characters - or at least 8 characters if it is to be used on a system processing nationally classified data.

20. An ideal way of creating secure passwords is by making them alphanumeric i.e. containing letters and numbers. In order to make the password easier to remember a hidden meaning may be added:

"SASO6P"	Sing a song of six pence;
"967PIMB"	967 pages in my book;
"672FSITR"	672 files in the registry;
"26WITBO"	26 windows in the building opposite;
"TA9COHCR"	There are 9 chimneys on Hampton Court roof;

21. Secure passwords may also be created by linking two dictionary words together with a non-alpha character:

"HAPPY-DAYS"
"CAT*MOUSE"
"CAR_GAME"
"AND?OR"
"FULL.STOP"

22. Even names may be made secure if extra characters are added or simple changes made:

"?NDREW"	
"ENNAANNE"	(Backwards and forwards);
"GE0RGE"	(With a zero instead of an "O");
"SAM-AN-THA"	
"TARGAREM"	(First and last letters switched);
"(JOHN)"	
"WSTMNSTR"	(Vowels removed).

23. Users may also consider using dates that have a particular significance for them (other than obvious ones like birthdays, which might be known to others). For added security differing formats can be used:

"070777"	"JUL7,77"
"7-7-77"	"7JULY1977"
"7:7:1977"	"JUL7th,77"
"7/7/77"	

24. Instead of trying to choose a password that is easy to remember, users can select a password where it is easy to remember how it was created:

"IWLAAC"	the initials of the first line of Wordsworth's poem "Daffodils".
"ADGJL:"	every other key on the middle line of the keyboard, but beware using every key on any particular line e.g. "QWERTY".
"UDTQCSSHND"	initials of the French words for the numbers 1 - 10.
"1992SPAIN"	A memorable holiday.
"2A6S0S7"	A mix of extension number and initials.

Changing:

25. The longer a password remains unchanged, the more opportunity a potential intruder will have to discover it. Once compromised a password will continue to give an intruder access to a system until such time as it is changed. An essential countermeasure is therefore to ensure that the password is changed regularly. In so doing it would be counter-productive if a previous password were to be used again. Thus staff should aim to invent a new and unique password each time a change is necessary.

26. Where a system automatically reminds users that a password is due to be changed, but does not enforce the change, (as some do), the change should be made as soon as possible. If the system allows the user to decide when

to change the password it should be so changed at least every 3 months unless the system manager decides that it should be made at other intervals. If the data on the system are sensitive it may be advisable to change the password more frequently.

[NOTE: It is not advisable to change a password on a Friday afternoon or just before a prolonged absence from work, (e.g. on annual leave) as there is a good chance that it will be forgotten].

27. Lastly, passwords should always be changed immediately there is the slightest suspicion that they or the system has been compromised in any way.

For further information relating to computer security matters please contact the Force Information Security Manager, telephone 2704.

B Protective Marking Guidance

The application of ‘need-to-know’ is fundamental to all aspects of security. Where it is necessary to reinforce ‘need-to-know’, special handling instructions may be applied.

If material is originated requiring a protective marking, a descriptor may be added to reinforce ‘need-to-know’ by indicating the nature of an information asset’s sensitivity and the need to limit access to it. Its use indicates to others the nature of the threat and the interested groups that may be given access.

Where there is a statutory requirement for access or disclosure of information, the use of a protective marking, with or without a descriptor, on information will not exclude the required access to that information. Where the information is covered by an exemption to the access rights and consequently should not be made available, this should be signalled by marking the relevant documents: NOT FOR DISCLOSURE with a reference being made to the appropriate act and reason for exemption by the originator.

Information marked with a descriptor should in the first instance be handled and protected in accordance with its protective marking. The application of a descriptor is only intended to highlight a need to take additional common sense precautions to limit its access to individuals and interested groups authorised to see it.

Originators must not generate their own descriptors. Only the descriptors listed below may be used.

APPOINTMENTS

Concerning actual or potential appointments that have not yet been announced.

COMMERCIAL

Relating to a commercial establishment’s processes or affairs.

CONTRACTS

Concerning tenders under consideration and the terms of any tenders.

CRIME

Concerning Crime.

HONOURS

Recognition given for exceptional achievements.

INFORMANTS

Regarding informants and their handling.

Any informant related information should be protectively marked as a baseline CONFIDENTIAL, with the appropriate handling procedures. Information that identifies an informant may require marking as SECRET.

INVESTIGATIONS

Concerning investigations into disciplinary or criminal matters.

MANAGEMENT

Policy and planning affecting the interests of groups of staff.

MEDICAL

Medical reports and records and material relating to them.

PERSONAL

Material intended for the person to whom it is addressed.

POLICY

Proposals for new or changed government or Force policy before publication.

PRIVATE

Information collected through electronic government services provided to the public and relating to the individual:

- Access to be limited to the individual concerned and those representatives of agencies with a requirement for access under the governing legislation.

Information collected through electronic government services provided to the public and relating to an organisation:

- Access to be limited to the appropriate officials of the organisation concerned and by those representatives of agencies with a requirement for access under the governing legislation.

STAFF

Concerning references to named or identifiable staff or personal confidences entrusted by staff to management.

VISITS

Concerning details of visits by, for example, royalty, ministers or very senior staff.

With the exception of PERSONAL and PRIVATE, which may be used by themselves, the above descriptors may only be used in conjunction with a protective marking.

B.1.1 Handling, Transmission and Storage of Information Assets

Paper Documents		
	RESTRICTED	**CONFIDENTIAL**
Marking of Information	Top and bottom of every page; pages numbered	Top and bottom of every page; pages numbered.
Storage of paper	Protected by one barrier, for example, a locked container.	Protected by two barriers, for example, a locked container in a locked room.
Disposal of papers	Secure waste sacks **Keep secure when left unattended.**	Tear by hand and place in secure waste sacks or use a cross cut shredder **Keep secure when left unattended**
Data		
	RESTRICTED	**CONFIDENTIAL**
Force Data Network	May be used	May be used in conjunction with in accordance with your

		accreditation status
Criminal Justice Extranet	May be used	Encryption must be considered in accordance with the recommendations from the Manual of Protective Security
Internet	Government approved encryption required. Contact Force Information Security Manager	Not to be used.
Fax	Check recipient is on hand to receive. Send cover sheet first and wait for confirmation before sending.	Use a secure fax machine only.
Disposal of magnetic media	Return to Technology Unit	
Voice		
	RESTRICTED	**CONFIDENTIAL**
Mobile telephones	Digital cell phones may be used. This does not include cordless telephones.	Only if operationally urgent; use guarded speech and keep conversations brief.
Message Pager Systems	Not to be used due their inherent insecurity	Not to be used

If there is a requirement to use any of the above methods of communication to pass information at a higher level than it is recognised safe to do so, the operational urgency and the need for transmission must be weighed against the risk of a security breach, for which you and/or the Force may be held accountable. If it is decided that such transmissions are essential they should be kept short and guarded speech used. The use of some form of prearranged codes should be considered to avoid identifying officers, informants or locations

B.1.2 MOVEMENT OF PROTECTIVELY MARKED MATERIAL

RESTRICTED		
WITHIN THE CoLP	**WITHIN GREAT BRITAIN**	**OUTSIDE GREAT BRITAIN**
By trusted hand; OR Via the internal despatch service in a sealed envelope, or other container, with the protective marking and descriptor visible. Transit envelopes may be used, but must be sealed with the appropriate security label.	By trusted hand in a closed envelope or container; OR By post, or courier service. If so sent, the envelope should show no protective marking or descriptor (other than PERSONAL, if appropriate). It should be addressed to an individual by name or appointment	By trusted hand in a sealed envelope or secured container; OR By post or courier service. If so sent, the envelope should show no protective marking or descriptor (other than PERSONAL, if appropriate) It should be addressed to an individual by name or appointment. Contact SB for details of countries of special sensitivity

CONFIDENTIAL		
WITHIN THE CoLP	**WITHIN GREAT BRITAIN**	**OUTSIDE GREAT BRITAIN**
By trusted hand; OR Via the internal despatch service in a new sealed envelope, or other container, with the protective marking and descriptor visible Transit envelopes must not be used	By trusted hand in a sealed envelope or secured container **OR** By post, or courier service, using double envelopes as described below.	Secured Container or double envelopes (see below) Contact SB for details of countries or special sensitivity.

	OUTER ENVELOPES, or secure containers, should not show the protective marking or descriptor, but should show the name/appointment and address of the recipient and a return address. Inner ENVELOPES should be similarly addressed and marked CONFIDENTIAL (plus DESCRIPTOR, if any

NB: "By trusted hand" means always in the possession of an employee or contractor with a security clearance appropriate for uncontrolled access to the material; the internal despatch service does not meet this requirement.

SECRET		
WITHIN THE CoLP	**WITHIN GREAT BRITAIN**	**OUTSIDE GREAT BRITAIN**
By trusted hand; OR The internal despatch service must not be used. Movement sheets required.	Secured container or double envelopes (see below) To be carried only by trusted hand. Receipts and movement sheets are required.	Double envelopes (a secured box, or bag, or pouch will count as outer envelope). If an approved tamper evident envelope is not used as outer envelope, the inner envelope should be security sealed. Diplomatic Protection required or (for bulky items carried in hold) escort to and from aircraft on direct flight. Receipts and movement sheets are required
OUTER ENVELOPES, including secure bags or pouches, should not show any protective marking or descriptor, but should show the name/appointment and address of the recipient and a return address. INNER ENVELOPES should be similarly addressed and marked SECRET (plus DESCRIPTOR, if any).		

TOP SECRET		
WITHIN THE CoLP	**WITHIN GREAT BRITAIN**	**OUTSIDE GREAT BRITAIN**
By trusted hand. The internal despatch service must not be used. Movement sheets are required	Double envelopes (a secured box or bag or pouch will count as outer envelope). If an approved tamper evident envelope is not used as outer cover, the inner envelope should be security sealed. To be carried only by trusted hand. Receipts and movement sheets are required	Double envelopes (a secured box, or bag, or pouch will count as outer envelope). If an approved tamper evident envelope is not used as outer envelope, the inner envelope should be security sealed. Diplomatic Protection required. Receipts and movement sheets are required.
OUTER ENVELOPES, including secure bags or pouches, should not show any protective marking or descriptor, but should show the name/appointment and address of the recipient and a return address. INNER ENVELOPES should be similarly addressed and marked TOP SECRET (plus DESCRIPTOR, if any) and include the inscription TO BE OPEND ONLY BY…(addressee or other designated person; or return to sender).		

Page 243

NB: "By trusted hand" means always in the possession of an employee or contractor with a security clearance appropriate for uncontrolled access to the material; the internal despatch service does not meet this requirement.

C The Law and electronic communications

The Data Protection Act 1998

The Data Protection Act 1998 (DPA) requires departments and agencies to process personal data 'fairly' and 'lawfully'.

Personal data means information about identifiable living individuals and includes both facts and opinions about the individual. The DPA provides for individuals to be provided with a copy, on request, of the personal data an organisation holds on them.

The DPA does not just apply to data held on large databases. Any set of data held electronically, including material held on a personal computer, is potentially disclosable. This includes any references to an individual in any document, file, folder or e-mail, including e-mails still in the "deleted" folder.

Although there has been a tendency to consider e-mails as an informal or ephemeral way of communicating, the data they contain is subject to the same disclosure provisions as data elsewhere. Directories containing names, telephone numbers, e-mail addresses, etc also fall within the scope of the Act. The DPA also applies to certain collections of non-computerised personal information, such as printouts of e-mails held in structured filing systems. It is crucial to ensure that anything created is accurate, relevant and justifiable, and that data and e-mails no longer necessary for business are fully deleted.

You can obtain further information from the Data Protection Officer (ext. 2209). Further information can also be found on the Home Office site at: http://www.homeoffice.gov.uk/foi/foidpunit.htm or the Information Commissioner's web site at: www.dataprotection.gov.uk. You should note that policy responsibility for the Data Protection Act transferred from the Home Office to the Lord Chancellor's Department (LCD) in June 2001. The links above may also be expected to change.

C.1.1 Human Rights Act 1998

The Human Rights Act 1998 incorporated the European Convention on Human Rights into domestic law. Under this Act a UK citizen is be able to assert their Convention rights through the national courts without having to take their case to the European Court of Human Rights.

Further information on the Human Rights Act can be found on the Home Office site at: http://www.homeoffice.gov.uk/hract/hramenu.htm

C.1.2 Regulation of Investigatory Powers Act 2000

Part I of the Regulation of Investigatory Powers Act 2000 (RIPA) makes it unlawful for employers and others to intercept communications, in the course of their transmission on a private telecommunications system, unless certain conditions are met. Interception is allowed where: -

- the parties to the call, e-mail or other communication have both consented to the interception, or
- the interception is of communications taking place using the employer's business telecommunications system and is authorised under The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

The RIPA only restricts access to the contents of a communication. It does not address the collection and use of traffic data on a private network, for example, the information about telephone calls that would typically be produced by a call logger. This is subject only to the requirements of the Data Protection Act 1998.

A public sector employee invoked the European Convention on Human Rights after her employer intercepted her telephone calls (Halford v UK Government). The European Court of Human Rights found that the secret interception of calls made by Ms Halford from her office amounted to an unjustifiable interference with her right to respect for her privacy and correspondence, contrary to Article 8(1) of the European Convention on Human Rights.

Further information on RIPA can be found on the Home Office site at: http://www.homeoffice.gov.uk/ripa/ripact.htm

C.1.3 The Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000

The Lawful Business Practice Regulations authorise certain interceptions of communications that would otherwise be prohibited under the RIPA 2000. The interception has to be by or with the consent of a person carrying on a business (which includes the activities of government departments, public authorities and others exercising statutory functions), for purposes relevant to that person's business, and using that business's own telecommunication system.

Interceptions are authorised for:

- monitoring or recording communications -
  - to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training),
  - in the interests of national security (in which case only certain specified public officials may make the interception),
  - to prevent or detect crime,
  - to investigate or detect unauthorised use of telecommunication systems, or
  - to secure, or as an inherent part of, effective system operation;

- monitoring received communications to determine whether or not they are business communications;
- monitoring communications made to anonymous telephone help lines.

Interceptions are authorised only if the controller of the telecommunications system on which they are affected has made all reasonable efforts to inform potential users that

interceptions may be made. The Regulations do not authorise interceptions to which the persons making and receiving the communications have consented: they are not prohibited by the Act.

Further information on the Regulations can be found on the DTI web site at:
http://www.dti.gov.uk/cii/regulatory/telecomms/telecommsregulations/lawful_business_practice_regulations.shtml
The Regulations are available on the HMSO web site at: http://www.legislation.hmso.gov.uk/si/si2000/20002699.htm

C.1.4 The Freedom of Information Act 2000

The Freedom of Information Act (FOI Act) gives a general right of access to information held by the force. In due course it will replace the existing Code of Practice on Access to Government Information. The Act also amends certain provisions of the Public Records and Data Protection Acts. It provides clear statutory rights for those requesting information together with a strong enforcement regime. Under the terms of the Act, any member of the public will be able to apply for access to recorded information held by bodies across the public sector.

> *The legislation will apply to a wide range of public authorities, including Parliament, Government Departments and local authorities, health trusts, doctors' surgeries, publicly funded museums and thousands of other organisations.*

The Act gives a general right of access to information held by public authorities in the course of carrying out their public functions, subject to certain conditions and exemptions.

Together these Statutes place a duty on departments and agencies to manage records, including e-mails, in such a way that their provisions can be complied with.

Further information can also be found on the Home Office site at: http://www.homeoffice.gov.uk/foi/foidpunit.htm or the Information Commissioner's web site at: www.dataprotection.gov.uk.

C.1.5 Obscene Publications Act 1959

All computer material is subject to this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it.

A computer disk, including the principal hard disk of the computer, can constitute an obscene article for the purposes of this Act if it contains or embodies matter that meets the test of obscenity. 'Publish' has a wide meaning and is defined as including distributing, circulating, selling, giving, lending, offering for sale or for lease. It seems clear that material posted to a newsgroup or published on a World Wide Web page falls within the legal definition of publishing and is therefore covered by the Act. The publisher would appear to include the originator or poster of the item.

C.1.6 Telecommunications Act 1984

The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under s.43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

C.1.7 Protection of Children Act 1978; Criminal Justice Act 1988

These Acts make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent.

C.1.8 Copyright, Design and Patents Act 1998

Copyright law applies equally to the Internet as it does to paper material. Many web sites contain a copyright notice detailing how the material they contain may be used. Often, this is in the form of a hyperlink from a short copyright notice to a more detailed statement of

what is permitted. If no copyright notice is provided, it is not safe to assume anything. If you want to print out a Web page or attachment, or copy-and-paste anything from a Web page or attachment into a document of your own, you should obtain the permission of the copyright owner. For any use beyond everyday Web-browsing, permission should be obtained. A good starting point is to send an email to the web site operator. Where permission has not been granted, individuals and the Commissioner could be liable to civil proceedings by the author.

C.1.9 Protection from Harassment Act 1997; Sex Discrimination Act 1975; Race Relations Act 1976

Harassment and discrimination are unlawful, whether or not the use of work-based communications facilities has played a role.

C.1.10 Computer Misuse Act 1990.

This Act makes it an offence for an unauthorised person to access knowingly a program or data or for such a person to modify knowingly the contents of a computer.

This is not a comprehensive list of the law that could be relevant. Anyone requiring specific information on the effects or the effective implementation of these Acts should seek advice from an appropriate legal source.

D Data Cleansing Request Form

Device Information (to be completed by the source department)

Device location: _____

(include department, building and floor)

Device Type: ☐ Computer ☐ USB Drive ☐ Server HDD
☐ Laptop ☐ Printer ☐ Photocopier HDD
☐ Other (Please specifiy) _____

Manufacturer: _____ Model: _____

Serial Number: _____ Property Tag ID: _____

I authorise the above device to be decommissioned in accordance with the Force Asset Disposal procedure and can verify that any CoLP information has been removed from the device.

Name: _____ Position: _____

Signature: _____ Date: _____

Cleanse Verification (to be completed by Technology Unit)

Decommission date: _____ Date of Cleanse: _____

Method of Cleanse: ☐ Software ☐ Physical Destruction ☐ Degaussing ☐ External Service

Details of Cleanse:

(Include brief details of work undertaken including software or service provider)

Equipment location: _____

I confirm that the details entered on this form are a true and accurate record.

Name: _____ Position: _____

Signature: _____ Date: _____

A copy of this form must accompany the equipment when sent to IT for disposal. On finalisation the completed form must be sent to the Force ISO for audit purposes.

Last revision date 20/05/08

E Third Party Connection Agreement

EXAMPLE AGREEMENT FOR A THIRD PARTY USER FOR CONNECTION TO A FORCE IT SYSTEM

1 This agreement between the City of London Police and

Hereinafter referred to as the USER, relates to the USER's connection to the following system(s):

2 The connection is subject to the terms and conditions set out in Schedule 1 (attached).

3 The type or method of connection will be by:

4 The following list of specific items of user equipment and software are approved by the Force for connection to the system:

5 The USER is permitted connection for the following purposes:

6 The USER is permitted to access the following information:

7 The USER is permitted to disclose the following information:

#Third Party Company#

Signed: _____ Date: _____

Position:

City of London Police (Information Asset Owner)

Signed: _____ Date: _____

Position:

SCHEDULE 1

INTRODUCTION

1. This Schedule sets out the terms and conditions under which the City of London Police provides an authorised third party, hereafter called the User, with a connection to the specified computer system.

2. The system may contain protectively marked information which **must** not be disclosed to unauthorised individuals or organisations. It is therefore essential that it should be adequately protected from all security threats which may result in:

    - reductions in systems reliability and performance;
    - inaccurate or incomplete data; or
    - unauthorised disclosure of protectively marked data.

    It is therefore necessary that the security of the system should not be compromised as a result of the connection of independent organisations to any part of the system.

3. It is a condition of access to the system that the User should maintain at least the minimum system security controls as set out in this Schedule.

RIGHTS AND OBLIGATIONS

4. Whilst it is the responsibility of the User to implement the minimum security controls described in this Schedule, they should not necessarily regard them as sufficient to meet the User's own security requirements, e.g. under the Data Protection Act.

5. The City of London Police reserves the right either:

to audit the relevant security controls implemented by the User against the requirements set out in this schedule at reasonable and convenient times. Such audits may be arranged at short notice and may be carried out by the City of London Police or by other qualified organisations authorised by the City of London Police to act on its behalf;

or

to request that a suitable annual audit be carried out by the User at the User's expense.

The execution and findings of audits carried out by or on behalf of the City of London Police will be recorded. When corrective action is required the record will be made available to the User. The User will be required to submit a written annual statement to the City of London Police confirming that his security controls are in compliance with this Schedule.

6. If an audit reveals a security weakness which, in the opinion of the City of London Police, is not in compliance with this Schedule, or which in any other way unnecessarily exposes the system to a security risk, then the user will be asked by the City of London Police to implement appropriate improvements.

7. The City of London Police reserves the right to discontinue User access to the system if, in its opinion, User security procedures are inadequate. In these circumstances User access may be restored following a satisfactory formal audit of any security improvements that are required.

8. The City of London Police reserves the right at his sole discretion to permanently disconnect a User from the system for whatever reason and such disconnection shall not give rise to any claim for damages or compensation of any kind whatsoever by the User or by any third party claiming or purporting to claim through the User.

9. The User is responsible for protecting the confidentiality of information obtained from the system.

10. Information made available to the User under the Agreement has been compiled to satisfy the City of London Police's requirements. Although all reasonable efforts are made to ensure its accuracy and completeness, the City of London Police will accept no responsibility for any inconvenience or loss or damage resulting from the User's reliance upon this information for other purposes, or from any interruption in system service which may be necessary.

11. The User is responsible to the City of London Police for the consequences of any breach of system security which is occasioned by the User's staff.

MINIMUM SYSTEM SECURITY CONTROLS TO BE IMPLEMENTED BY USER

12. Throughout the following, the term 'User equipment' includes any computer equipment on the User's premises or under the User's control, which is or is intended to be connected to the system. The User equipment and associated software shall be as defined in Item 4 of the Agreement.

SECURITY ADMINISTRATION AND STAFFING

13. The City of London Police will appoint a person or persons ("the City of London Police's nominated representative") to oversee the implementation by the User of the provisions of this Schedule relating to security controls to be enforced, maintained and monitored by the User.

14. The User will appoint a suitably qualified and authorised member of staff (the "security administrator") to be formally responsible for enforcing, maintaining and monitoring the security controls set out below. The security administrator will be responsible for ensuring that all necessary records and documentation are current and complete, and for liaising with the City of London Polices' nominated representative on matters relating to the security of the connection to the system

and associated equipment and facilities. These responsibilities must be formally documented, with appropriate reference to the Agreement.

15. The User equipment will only be operated by suitably qualified and trained members of the User's staff. The City of London Police reserves the right to carry out such security vetting checks on the members of staff which they may, at their sole discretion, consider necessary to safeguard the security of systems.

16. The User must place a formal responsibility on members of staff to adhere to all system security controls and procedures. Members of the User's staff must be informed of this responsibility in writing.

SECURITY OF EQUIPMENT

17. Only the specific equipment identified in the Agreement may be connected to the system.

18. A register must be kept of all normal use made of the User equipment and must include:

a) the dates and times of the beginning and end of each period of physical connection;
b) the purpose of the use;
c) details of all User log-ons and log-offs; and
d) the name(s) of the staff involved.

19. The User must comply with system password and other access control procedures stipulated by the City of London Police.

20. No User equipment connected to the system may concurrently be connected to any other computer or communication system without the prior agreement of the City of London Police. Any connection between the User equipment and other

computers or networks which the User may make from time to time must be recorded in a log which must include:

a) the dates and times of the beginning and end of the physical connection period; and

b) the purpose of the connection.

21. All system and User logs stipulated in this Schedule must be made available for audit when required.

PHYSICAL ACCESS SECURITY

22. Physical access controls to User equipment must be in accordance with methods agreed with the City of London Police and be in operation at all times to ensure:

a) only authorised members of User staff operate the equipment; and

b) all unauthorised staff, such as equipment maintenance personnel and office cleaning personnel, who require occasional access to User equipment or its accommodation, are supervised, at all times, by an authorised member of staff.

OPERATIONS AND DATA SECURITY

23. User equipment will only be connected to the system at times and for periods agreed with the City of London Police's nominated representative. Specialised User equipment connected for technical support purposes will normally only be connected to the system at times and for periods necessary for the purpose, and in all cases with the explicit prior permission of the City of London Police's nominated representative.

24. Any data other than that permitted by the City of London Police for disclosure which is retrieved by User equipment from the system in permanent form (whether in printed or electronic form) must be retained within the same physical

environment and destroyed after use. Destruction shall be by non-recoverable means (e.g. shredding or incineration).

25. Computer terminals must be positioned to avoid the possibility of casual observation by unauthorised persons.

26. The User must take precautions to protect the confidentiality of any documentation relating to the system.

27. Information for which disclosure has not been permitted is subject to the provisions of the Official Secrets Act. The User shall produce a sign to remind the User's staff of the Act and its applicability, and erect copies in the appropriate areas.

F Security Incident Reporting

You can create a new security incident report by clicking here or navigating to SharePoint and selecting “Report Security Incident” from the home page.

Security Incidents are broken down into the following categories and should be reported in all instances here.

Email Misuse

- Emailing information to a non-secure address (via an insecure route) (E.g. Home PC’s)
- Sending inappropriate content in contravention of local policy
- Emailing information assets to unauthorised recipients

ID Cards – Keys – Warrants:

Lost - Missing – Stolen – Not Returned.

- Includes access control tokens
- Those that can be disabled
- Those where there is a continuing risk

Physical Security

Wide ranging but consider local policy and:

- Failed locks
- Doors wedged open – windows left open
- Door combination settings unofficially shared with unauthorised personnel
- Alarms not set

Airwave Incidents

- Radios Lost or Stolen
- Confirm stunning
- Breach of Procedures

Unplanned Outage

- Equipment failure
- Incidents where some action that was not expected to affect system availability did so
- System was taken out of service, but users were not told beforehand

Procedural

- Failure to comply with procedures through lack of awareness
- Deliberate attempts to circumvent security measures.

Unauthorised Disclosure

- Misconduct cases
- Data Protection Act breaches

- Information made available to people who are not authorised to have it
- Sensitive information on paper not securely disposed of

System Misuse

- Use of an ICT system other than for its intended authorised purpose such as an enquiry on PNC to satisfy private curiosity, rather than for a genuine investigation.

Malicious Software

- Successful and regular identification and quarantine of malware at or near a system boundary is **not** counted as an incident. Unusual or unexplained activity at a system boundary (e.g. potential denial of service attack) should be reported.

Unauthorised access to systems or data

- Access rights incorrectly granted
- Clear desk policy breaches
- Unattended equipment left logged on

Internet Misuse

- Breaches of Force policy
- Excessive personal use
- Disclosures on personal social networking sites

Unauthorised Person(s) on Premises

- Failure in Technical access controls
- Failure in physical access procedures

Account Sharing

- Password sharing, or an account signed on by one person and used by another / several.
- Non Standard Accounts

Loss or Theft of Technology Assets

- Laptop
- PDA
- Blackberry
- Mobile 'Phone
- USB Memory Sticks
- Portable peripherals
- Other Assets

Paper Documents

- Lost Including non-delivery by Royal Mail, courier, internal post
- Documents found where they should not have been
- Left insecure on desks, in cars, public transport etc.
- Breaches of GPMS

Crypto

- Any incident involving crypto.
- Breaches of IS4 requirements.
- Note that the loss or theft of any Crypto item should be reported using CINRAS.

Data Storage

- Where data – including backups - is not stored in accordance with its protective marking.

Vetting / Personnel

- New employee, contractor or volunteer, allowed access to premises or data without clearance.

Removable Media Related Incidents

- Use of private USB memory sticks to transfer data
- Unauthorised download / upload of data via USB ports
- Unauthorised download / upload via other media, e.g. CD's.

Social Engineering

- Masquerading as someone entitled to access to information or premises.

Unauthorised Equipment

- Use of equipment that has not been approved by the ICT department – generally items brought from home

Unauthorised Software

- Commercial software installed without authority / licence

Unauthorised System Connection

Insecure Disposal

- Breaches of IS5 requirements

Loss or Theft of Uniforms

Committee: Police Committee- For information	**Date**: 2nd November 2017
Subject: Capital and Revenue Budget Monitoring Report to September 2017	**Public**
Report of: The Commissioner of Police and The Chamberlain	**For Information**
Report author: Michelle King, City of London Police Director of Finance	

Summary

The overall forecast year end position at quarter two would require a draw down on reserves of £1.61m, this compares to the balanced position reported in quarter 1. However, the Home Office have confirmed National Lead Force funding of £2.195m is being made available for 2017/18, which removes one of the risks.

Chief Officer Cash Limited Budget

There are variances of £1.61m against the approved budget of £60.4m (excluding internal recharges of £3.6m). Brief commentary on the main variances and mitigating actions being undertaken are outlined in Appendix 1.

Recommendation

Members are asked to note the report.

Chief Officer Cash Limited Budget

1. Variances arising in quarter two without mitigation identifies a forecast overspend of £1.61m, this is a deterioration from the balanced position reported in quarter 1. The Home Office have settled the outstanding issues on National Lead Force funding in favour of CoLP. The updated position per Directorate is shown below in table 1.

Table 1: Directorate Outturn at Summary Level

Directorate	Budget £m	Q2 Actual £m	Forecast Outturn £m	Better/(Worse) £m
Crime	11.03	4.90	10.69	0.34
ECD - Core Units	5.52	2.74	5.43	0.09
ECD - Funded Units	2.10	9.54	2.10	0.00
I&I	11.01	4.62	10.76	0.25
UPD	10.79	6.51	10.68	0.11
BSD	14.65	6.85	14.76	(0.11)
Central Budgets	5.30	(14.22)	7.59	(2.29)
Total Net Expenditure	60.40	20.94	62.01	(1.61)

Revenue

2. The adverse variances identified at quarter two of £1.61m are shown in more detail in Appendix 1. The main adverse variances are in relation to issues around the failure to identify savings in the non-pay Chief Officer Cash Limited Budget of £0.87m, the overtime costs incurred as a result of the terrorist events of £0.45m and the impact of the pay awards above that which had been provided of £0.37m.

3. Chief Officer Cash Limited Budgets include a savings target of £1.2m against the non-pay budget of £29.3m. The force has managed to secure savings of £0.33m against Repair and Maintenance, Travelling Expenses, Tasking and Core Directorate Overtime Budgets; however, this falls short of the savings target by £0.87m. As reported in quarter one this target and the update remains unchanged.

4. Unplanned savings in direct employee pay have continued to accrue to quarter two to show a revised position of £0.96m.

5. Exceptional overtime claims relating to terrorist activities (Westminster attack, London Bridge and Manchester Arena) paid to officers to date amount to £0.45m, this shows a slight reduction on the figure forecast in quarter one of £0.03m. The claim submitted to National Counter Terrorism Policing Head Quarters (NCTPHQ) for approval, remains outstanding.

6. The Injury and Ill Health commutations year end forecast is £0.26m worse than the latest approved budget of £0.7m. This continues to be monitored and has not changed since quarter one.

7. The adverse variance in relation to legal costs has risen slightly in quarter two by £11k to £218k. This negative variance is still anticipated to increase by year end due to the outcomes of further court actions, the value of which will continue to be monitored and reported throughout the year.

8. In light of these variances, the current best estimate of forecast is a £1.6m draw down of reserves at the year end. The pressures and on-going risks will be monitored as an agenda item at Force Strategic Finance Board.

9. The £395k savings identified within the Deloitte "quick wins" are not factored in but are intended to be used in year to fund the Review change team, subject to Members and Chief Officer's approval.

10. The achievement of the "efficiency" savings target is at present proving to be extremely challenging in light of the increased terror threat and the impact on both pay and non-pay budgets. The force will continue to seek opportunities to address this issue.

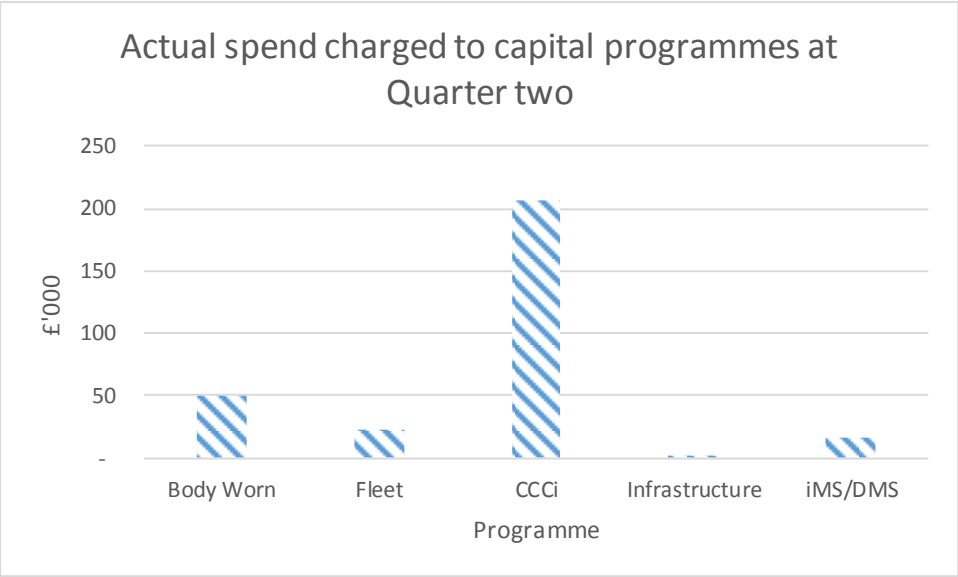
Proceeds of Crime Act 2002 (POCA)

11. Appendix 2 shows a summary of the actual spend for the second quarter against budgets agreed by the Strategic Management Board.

Capital and Supplementary Revenue Budgets

12. The capital outturn for 2017/18 has been profiled to budget. The ESN programme (formally ESMCP) is under review and was reported in quarter one and an update for quarter two is provided below. The analysis of actuals charged to capital as at quarter two are shown in table 2 below. An explanation of variances will be presented in the quarter three report.

Table 2 Actual spend to date on current capital programmes.



13. The Police submitted four bids to the Police Innovation Fund of which one bid "PR097- 2017 National to Local Fraud and Cyber Data Sharing" received a

recommendation to be considered by the Home Office (The bid value is £1.8m in 2017/18; £1.4m in 2018/19 and £0.5m in 2019/20). The bid was deferred from being submitted for ministerial sign off until September, as the Home Office wanted assurance that a current commercial dispute between the Force and one of its suppliers would not impact upon delivery. The Force has provided that assurance. There is nothing further to update the Committee at this point in time.

Major Programmes

14. There are several ongoing major programmes within the Police that are interdependent with the Corporation. These are Action Fraud, the Planned and Cyclical Maintenance of the Police Estates and the Emergency Services Mobile Communications Programme.

15. **Action Fraud**: The supplier has communicated a number of delivery delays to the Implementation Programme Board (IPB) following the initial service Go Live date of 1 April 2016. A further delay to Go Live for Release One has been communicated, with the current plan referring to 31st December 2017. Members should note that Release One will deliver all of the promised functionality to law enforcement and wider Stakeholders. Notwithstanding delays the system has been built and has been demonstrated on a number of occasions, the Home Office user acceptance testing (UAT) team have commenced early UAT with a view to streamlining the formal UAT process. Members approved a supplementary budget of £5.51m for 2017/18 to meet Milestone, Client Team and Legal advice costs relating to the on-going delivery dispute. To date £7.2m has been paid to the supplier for Milestones delivered with a further £2.9m budgeted. There have been no material developments in respect of the on-going dispute.

16. **Planned and Cyclical Maintenance of the Police Estate:** As at quarter two there are no significant issues to report on since the update provided in quarter one

17. **The Emergency Services Network programme:** Further to the position reported in quarter one, recruitment is ongoing and briefing to Members is being arranged. Final financial and staffing model is being prepared for Committees in November or December 2017. Due to its scale and complexity the Gateway process has been identified as problematic and a meeting is taking place with the Corporation to discuss the route through committees and best way to deliver governance and approval of the programme.

18. **Other Police Funds**

The forecast Police working balances includes the General fund £3.4m, the POCA reserve £0.9m and the transformational fund £0.1m as table 2 outlines.

Table 3: Other Police Funds Forecast to March 2018

Forecast Other Police Funds to 31st March 2018	2017/18 Opening Balance £m	2017/18 Projected Drawdown £m	2017/18 Closing Balance £m
General	3.5	(1.6)	1.9
POCA	3.6	(2.7)	0.9
Transformational Funding	0.1	-	0.1
Total Other Police Funds	7.2	(4.3)	2.9

Appendix 1 – Budget Variances as at Quarter two
Appendix 2 - POCA Allocations for 2017/18
Appendix 3 – Capital and Supplementary Revenue Budget

Contacts:
Michelle King
0207 601 2411
Michelle.King@cityoflondon.pnn.police.uk

Appendix 1

Budget Variances as at Quarter Two

Changes	Q1 Risks £'000	Movement £'000	Q2 Risks £'000	Cause/Action
Direct Employee Pay	600	355	955	Adjustments to direct employee costs due to revised recruitment profile resulting from vacant positions. The under spend will be taken to the Police Contingency Fund to offset the underachievement of non-pay efficiencies. The position is as at quarter two, however with the current recruitment campaign this efficiency will have to be continually monitored to ensure that the non pay efficiencies can be covered.
Indirect Employee Pay	(482)	30	(452)	Adjustments to employee indirect pay due to terrorist attacks across the country. These costs have been reclaimed through the Counter Terrorism funding stream however NCTPHQ is uncertain about the likelihood of recovery and the status of this risk will be updated in quarter three.
Legal costs	(207)	(11)	(218)	These are adjustments relating to legal fees, interest and court costs paid to third parties relating to negative outcomes on forfeiture cases. The Assistant Commissioner is developing a process to risk assess and mitigate where feasible forfeiture risks prior to engagement. This will be updated to members in quarter three.
Non-pay efficiencies	(871)	0	(871)	The in year efficiencies are partially achieved where operationally feasible. The remaining non-pay savings are currently unidentified however in view of the high level of vacancies and the time to fill; these efficiencies will be offset against unplanned savings from direct employee budgets.
Injury and Ill Health Commutations	(260)	0	(260)	The current levels of Injury and Ill Health costs are forecast to exceed that budgeted for 2017/18 due to the provision of three commuted ill health lump sum and an increase in 4 weekly payments for injury awards.
National Lead Force	(2,195)	2,195	0	Confirmation received from the Home Office that this funding will be made available, hence no longer reported as a risk.
ATOC	0	(147)	(147)	The additional tax Liability for 2016/17 as reported to members at the last Police Committee
Additional Fees	0	(250)	(250)	The current assessment subject of a confidential report to the last Police Committee.
Pay award	0	(370)	(370)	This is the impact of the revised payaward taking account of costs over the 1% provision and the additional 1% bonus payment for Officers
	(3,415)	1,802	(1,613)	

POCA Reserve Allocations 2017/18

POCA - 2017/18 **Indicative Allocations: Strategic POCA Priorities**			
Allocation	POCA Allocation 2017/18 £'m	Actuals to Sept 17 2017/18 £'m	Allocation Remaining 2017/18 £'m
POCA Costs for ARTS/SARS Teams	1.21	0.46	0.75
Skynet Intelligence Hub	0.16	0.08	0.08
PCSO to June 2017	0.06	0.04	0.02
Operational Programmes	0.16	-	0.16
Voluntary Sector	0.04	0.04	-
Capital Programmes	1.04	0.53	0.51
	2.67	1.15	1.52

Capital and Supplementary Revenue Budget

Expenditure				
Programme	**17/18 Approved £'000**	**17/18 Pipeline £'000**	**RAG Budget**	**RAG Time**
ICT Support to CCCI Functions	(2,633)		Red	Red
Joint Network Refresh	(1,037)		Green	Amber
HR Origin Upgrade to R12	(55)		Green	Green
ROS - IMS/DRS (back office)	(683)		Green	Red
ESMCP		(4,000)	Red	Red
Infrastructure refresh IL4		(150)	Green	Amber
Unified Communications		(175)	Red	Red
Intranet upgrade		(100)	Amber	Green
Forensics Digital Laboratory		(38)	Amber	Amber
TFG Tasers and ancillary equipment		(50)	Amber	Amber
Payroll and Duty Management System		(300)	Amber	Green
Vehicle purchases		(298)	Green	Green
ROS - River Cameras		(453)	NA -frozen	NA – frozen
ROS - IMS/DRS		(357)	Green	Red
Subtotal Capital Expenditure	**(4,408)**	**(5,921)**		

Funding				
Programme	**17/18 Approved £'000**	**17/18 Pipeline £'000**	**RAG Budget**	**RAG Time**
Specific Projects Proceeds of Crime Funds - allocated to ICT support to CCCI functions	951		Green	Green
General Support				
Home Office Capital Grant	400		Green	Green
Police Control Room Grant		841	Green	Green
Revenue Contribution	1,378		Green	Green
On-Street Parking Reserve contribution to ROS - IMS/DRS		300	Red	Red
Bridge House Estates contribution to ROS - River Cameras/IMS/DRS		581	Red	Red
Subtotal Capital Funding	**2,729**	**1,722**		

	17/18 Approved £'000	**17/18 Pipeline £'000**
Net Funding (Shortfall)/Surplus	**(1,679)**	**(4,199)**

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank