Public Document Pack

CITY OF LONDON

Information Technology Sub (Finance) Committee

Date:	**FRIDAY, 14 JULY 2017**
Time:	**1.45 pm**
Venue:	**COMMITTEE ROOMS - WEST WING, GUILDHALL**

Members: Deputy Jamie Ingham Clark (Chairman)
Hugh Morris (Deputy Chairman)
Rehana Ameer
Randall Anderson
Deputy Keith Bottomley
John Chapman
Tim Levene
Jeremy Mayhew
Deputy Robert Merrett
Sylvia Moys
James Tumbridge

Enquiries: **Alistair MacLellan**
alistair.maclellan@cityoflondon.gov.uk

Lunch will be served in the Guildhall Club at 1pm

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**
To agree the public minutes and non-public summary of the meeting held on 26 May 2017.

For Decision
(Pages 1 - 6)

4. **OUTSTANDING ACTIONS**
Joint report of the Town Clerk and Chamberlain.

For Information
(Pages 7 - 10)

5. **IT DIVISION UPDATE**
Report of the Chamberlain.

For Information
(Pages 11 - 22)

6. **COUNCIL TAX & BUSINESS RATES**
Report of the Chamberlain.

For Decision
(Pages 23 - 26)

7. **GDPR BRIEFING**
Report of the Chamberlain.

For Information
(Pages 27 - 38)

8. **WEBSITE UPDATE AND ACTION PLAN INCLUDING MEMORANDUM OF UNDERSTANDING BETWEEN THE IT DIVISION AND COMMUNICATIONS DIVISION**
Report of the Director of Communications and the Information Technology Director.

For Information
(Pages 39 - 46)

9. **OPEN MEDIATED WIFI PROVISION FOR GUILDHALL EVENTS**
Report of the Chamberlain.

For Information
(Pages 47 - 52)

10. **WORK PROGRAMME**
Report of the Chamberlain.

For Information
(Pages 53 - 54)

11. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**

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

13. **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

14. **NON PUBLIC MINUTES**
To agree the non-public minutes of the meeting held on 26 May 2017.

For Decision
(Pages 55 - 58)

15. **NON PUBLIC OUTSTANDING ACTIONS**
Joint report of the Town Clerk and Chamberlain.

For Information
(Pages 59 - 60)

16. **IT TRANSFORMATION PROGRAMME - UPDATE REPORT**
Report of the Chamberlain.

For Information
(Pages 61 - 68)

17. **IT MOBILITY STRATEGY**
Report of the Chamberlain.

For Decision
(Pages 69 - 76)

18. **NEW IT TARGET OPERATING MODEL**
Report of the Chamberlain.

For Information
(Pages 77 - 94)

19. **CUSTOMER RELATIONSHIP MANAGEMENT (CRM)**
Report of the Chamberlain.

For Decision
(Pages 95 - 106)

20. **AGILISYS CONTRACT NEGOTIATIONS MEMBERS WORKSHOP**
Report of the Chamberlain.

For Information
(Pages 107 - 116)

21. **IT DIVISION RISK UPDATE**
Report of the Chamberlain.

For Information
(Pages 117 - 142)

22. **SOCITM ASSURANCE COVERING REPORT**
Report of the Chamberlain.

For Information
(Pages 143 - 166)

23. **DEEP DIVE: CR16 INFORMATION SECURITY**
Report of the Chamberlain.

For Information
(Pages 167 - 204)

24. **CITY OF LONDON PSN CERTIFICATION VERBAL UPDATE**
The Chamberlain to be heard.

For Information

25. **IT SERVICE AND PERFORMANCE**
Report of the Chamberlain.

For Information
(Pages 205 - 208)

26. **SUPERFAST BROADBAND RESOURCE**
Report of the Chamberlain and the Director of Built Environment.

For Decision
(Pages 209 - 232)

27. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**

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

This page is intentionally left blank

Agenda Item 3

INFORMATION TECHNOLOGY SUB (FINANCE) COMMITTEE

Friday, 26 May 2017

Minutes of the meeting of the Information Technology Sub (Finance) Committee held at Guildhall, EC2 on Friday, 26 May 2017 at 11.00 am

Present

Members:
Deputy Jamie Ingham Clark (Chairman)
Hugh Morris (Deputy Chairman)
Rehana Ameer
Randall Anderson
Deputy Douglas Barrow
Deputy Keith Bottomley
John Chapman
Tim Levene
Jeremy Mayhew
Sylvia Moys
James Tumbridge

Officers:

Alistair MacLellan	-	Town Clerk's Department
Peter Kane	-	Chamberlain
Sean Green	-	Chamberlain's Department
Matt Gosden	-	Chamberlain's Department
Kevin Mulcahy	-	Chamberlain's Department
Gary Brailsford-Hart	-	City of London Police
Eugene O'Driscoll	-	Agilisys

1. **APOLOGIES**
   Apologies were received from Deputy Robert Merrett.

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

3. **APPOINTMENT OF SUB COMMITTEE AND TERMS OF REFERENCCE**
   Members received a resolution of the Finance Committee appointing the Sub Committee, setting its composition and terms of reference.

   The Chairman welcomed new Members on to the Sub Committee and noted his thanks to Members who had served during 2016/17 and who were now no longer on the Sub Committee.

   RECEIVED

   Rehana Ameer arrived at this point of the meeting.

4. **MINUTES**
The minutes of the meeting held on 22 February 2017 were approved.

5. **OUTSTANDING ACTIONS FROM PREVIOUS MEETINGS**
Members considered a joint report of the Town Clerk and the Chamberlain which provided updates of outstanding actions from previous meetings, and the following points were raised.

- The Member Survey would be conducted in October 2017 rather than November 2017. In response to a question, the IT Director replied that ongoing customer surveys were based on IT Helpdesk customer feedback and the annual outturn reporting.

- In response to a request the Town Clerk agreed to circulate the 2018 dates of the Sub Committee to Members.

RECEIVED

6. **WORK PROGRAMME FOR FUTURE MEETINGS**
Members considered a Joint Report of the Town Clerk and Chamberlain regarding the Sub Committee's Work Programme for 2017, and the following points were made.

- The IT Director noted that the Right to be Forgotten would come into effect from May 2018, and so would feature as an item at a future meeting of the Sub Committee.

- The Telephone Maintenance Contract had been awarded and so would not be referred to the Sub Committee in July 2017.

- In response to a question, the IT Director replied that the General Data Protection briefing due in July 2017 was to ensure that all Members of the Sub Committee were familiar with the issues involved in data protection.

- In response to a request from a Member, the IT Director agreed that future iteration of the Work Programme should be explicitly linked to corporate and departmental strategies.

- A Member noted she would be attending the International Conference of Data Protection & Privacy Commissioners in July 2017 and would provide a conference update to colleagues at the Sub Committee's next meeting.

RECEIVED

7. **IT DIVISION - MEMBER UPDATE**
Members considered an update report of the Chamberlain on the IT Division and the following points were made.

- The IT Director noted there was continued good progress in IT Transformation, with recent issues around hardware LAN procurement and LAN design and support. Overall service performance was considered good.

- The IT Director placed on record his thanks to Agilisys for its support to the City of London Corporation when responding to both the recent Westminster and Manchester terror attacks.

- The Town Clerk agreed to circulate the date of the IT Sub Members' Workshop outside of the meeting.

- The Chairman noted that the Sub Committee had requested a joint report of the Chamberlain and the City Surveyor regarding remediation responsibilities, but that the provision to Members of a memorandum of understanding between the two departments would suffice instead.

- In response to a question regarding Socitm Advisory, the IT Director noted that an interim report had been provided to the City of London Corporation. As a result of the report recommendations, a refreshed IT Division Operating Model would be implemented at the end of June 2017. Whilst Socitm Advisory recognised the complexity of the City of London, some recommendations on governance best practice had been put forward which were being reviewed by officers.

- The IT Director agreed to circulate the Socitm Advisory interim report to Members outside of the meeting.

- In response to a request the IT Director agreed to provide a one page dashboard detailing Risk Actions.

RECEIVED

8. **IT PERFORMANCE - MEMBER UPDATE**

Members considered an update report of the Chamberlain regarding IT performance and the following points were made.

- A representative from Agilisys noted that a number of upgrades were due imminently and that services would be available 24/7 from 1 June 2017.

- In response to questions, a representative from Agilisys confirmed that security audits had been conducted as planned during 2-4 May 2017, and the necessary certificates updated. Agilisys recognised more work needed to be done on security patching following the recent Ransomware incident.

RECEIVED

9. **OPEN MEDIATED WI-FI**

Members considered a Gateway 7 Outcome report of the Chamberlain on Open Mediated Wi-Fi. In response to a question regarding Wi-Fi provision at Guildhall events including the forthcoming Innovate Finance conference, the Chamberlain agreed to submit a report on the issue to a future meeting of the Sub Committee. In the meantime, Members were assured that the IT Division would continue to liaise with the Remembrancer's Events Team to ensure Wi-Fi provision at City events was satisfactory.

RESOLVED, that the Open Mediated Wi-Fi project be closed.

10. **CORPORATE DISASTER RECOVERY CENTRE**

Members considered and agreed a Gateway 7 Outcome report of the Chamberlain on the Corporate Disaster Recovery Centre.

RESOLVED, that the Corporate Disaster Recovery Centre project be closed.

11. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**

There were no questions.

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

Resolution of the Barbican Residential Committee regarding the City of London Corporation Website

Members considered a tabled resolution from the Barbican Residential Committee dated 13 February 2017. The resolution noted that Members of the Barbican Residential Committee felt that the search engine on the City of London Corporation website was not fit for purpose. The following points were made.

- The IT Director noted that he had discussed this issue with the Director of Communications, who was responsible for the team that managed the City of London Corporation's website and intranet. Consultants had been appointed to advise on improving user experience of the website and would report in June 2017. Following this, a report would be submitted to Members that would outline proposed improvements to the website.

- Members queried the split in responsibility for website system infrastructure and website maintenance between the IT Director and the Director of Communications, and expressed concern that this illustrated a disjoint in oversight. In response the Chamberlain agreed to bring a paper to the Sub Committee outlining service responsibilities and business requirements for the City of London Corporation website and intranet.

13. **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.

14. **NON-PUBLIC MINUTES**
The non-public minutes of the meeting held on 22 February 2017 were approved as a correct record.

15. **OUTSTANDING ACTIONS FROM NON-PUBLIC MINUTES OF PREVIOUS MEETINGS**
A joint report of the Town Clerk and Chamberlain on non-public outstanding actions since the last meeting was received.

RECEIVED

16. **IT DIVISION RISK UPDATE**
A report of the Chamberlain providing an IT Division Risk Update was received.

RECEIVED

17. **IT TRANSFORMATION PROGRAMME - UPDATE REPORT**
A report of the Chamberlain providing an update on the IT Transformation Programme was received.

RECEIVED

18. **IT TRANSFORMATION PROGRAMME WIDE AREA NETWORK PROGRESS UPDATE**
A report of the Chamberlain providing an update on the IT Transformation Programme Wide Area Network was received.

RECEIVED

19. **SUPERFAST CITY PROGRAMME UPDATE**
Members considered a report of the City Surveyor on the Superfast City Programme.

20. **RESOLUTION OF THE PROJECTS SUB COMMITTEE [10 MAY 2017]**
Members received a resolution of the Projects Sub (Policy and Resources) Committee dated 10 May 2017.

RECEIVED

21. **RANSOMWARE INCIDENT - BRIEFING NOTE**
Members received a report of the Chamberlain on the recent Ransomware incident.

RECEIVED

22. **CITY OF LONDON CORPORATION: 10 STEPS MATURITY ASSESSMENT**
The Chamberlain was heard regarding the 10 Steps Maturity Assessment.

23. **PATCHING REPORT**
The Chamberlain was heard regarding a Patching report.

RECEIVED

24. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE**
There were no non-public questions.

25. **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 non-public business.

The meeting ended at 12.59 pm

Chairman

Contact Officer: Alistair MacLellan
alistair.maclellan@cityoflondon.gov.uk

Information Technology Sub-Committee – Outstanding Actions

Agenda Item 4

Item	Date	Item and Action	Officer responsible	To be completed/ progressed to next stage	Progress update
	25 November 2016	Member Survey The Chamberlain to develop and analyse the results from the Members survey. Members to send in any additional remarks.	Peter Kane, Chamberlain's Department	November	More detailed research to be conducted following feedback and proposals brought to the first IT Sub Committee following the election.
	20 January 2017	IT Member Update Officers to provide a breakdown of workforce numbers of the previous years, including the levels pre-Agilisys for comparison to the current levels.	Sean Green, Chamberlain's Department	May	Completed
	22 February 2017	IT Member Update Report on the rationale behind the migration to Apple Devices be brought to the next meeting of the Sub-Committee.	Kevin Mulcahy, Chamberlain's Department	September	Update at July meeting
	26 May 2017	Outstanding Actions Town Clerk to circulate 2018 meeting dates to the Sub Committee.	Alistair MacLellan, Town Clerk's Department	May	Completed

Information Technology Sub-Committee – Outstanding Actions

	26 May 2017	GDPR GDPR Review to be added to Work Programme.	Sean Green, Chamberlain’s Department	July	Update at July meeting
	26 May 2017	Work Programme Work Programme items to reflect corporate and departmental strategies.	Sean Green, Chamberlain’s Department	July	Update at July meeting
	26 May 2017	IT Division Update Workshop Dates to be circulated to Members	Sean Green, Chamberlain’s Department	May	Completed 28th June 2017 10am-12pm
	26 May 2017	IT Division Update Memorandum of Understanding between IT Division and City Surveyor’s Department to be shared with Members.	Sean Green, Chamberlain’s Department	July	Update at July meeting
	26 May 2017	IT Division Update Socitm Interim Report to be shared with Members	Sean Green, Chamberlain’s Department	June	Update at July meeting
	26 May 2017	IT Division Update One page risk dashboard to be developed.	Matt Gosden, Chamberlain’s Department	July	Update at July meeting

Information Technology Sub-Committee – Outstanding Actions

	26 May 2017	IT Division Update Report on Wi-Fi provision for Guildhall Events to be submitted to the Sub Committee.	Matt Gosden, Chamberlain’s Department	July	Update at July meeting
	26 May 2017	IT Division Update Report on division of responsibilities between IT Director and Director of Communications for website/intranet to be submitted to the Sub Committee.	Sean Green, Chamberlain’s Department	July	Update at July meeting

This page is intentionally left blank

Committee(s)	**Dated:**
IT Sub Committee – For Information	14 July 2017
Subject: IT Division – Member Update	**Public**
Report of: The Chamberlain	**For Information**
Report author: Sean Green, IT Director	

Summary

The IT Division has maintained a focus on service availability whilst seeking to progress the transformation programme that will uplift the overall quality of IT services at the Corporation and City Police. Core updates:

- Service performance for the Corporation (CoL) and City of London Police (CoLP) was good with no P1's for CoLP and 2 P1 incidents for CoL.
- With the recent national incidents CoLP have had to enact the Casualty Bureau at short notice with the IT Service Desk and the IT Division providing IT support out of hours. The IT VIP team have also provided extended support to the newly established Westminster office for John Barradell who is leading the Grenfell Tower task force.
- The procurement activities for the LAN Hardware and services design, build and support was issued on the 7th June with a final submission date of 19th July. A decision on the tender award is expected by the end of July. Communications, presentations and roadshows are accelerating to support IT transformation, in particular the roll out of new devices and Office 365 with the CoL desktop transformation. Current IT change restrictions could impact the roll out timetable.
- CoLP Programme updates are provided in the body of this report. A business case will be prepared shortly for CoLP desktop transformation.
- A complete review of IT risks has been completed with a new heatmap presented in the risk report.
- Questions raised at the previous IT Sub Committee concerning:
  - The division of responsibilities between Facilities staff and IT staff with the Network remediation work currently underway covered in this report.
  - The division of responsibilities between Communications and IT for the management of the internet and development of the internet covered in a separate report for the IT Sub-Committee.
- A workshop with Members was held to review the approach and outcomes expected from the Agilisys contract extension negotiations.

Recommendation(s)

Members are asked to:

- *Note the report.*

Main Report

IT Service and Support

1. Customer satisfaction with City of London and City of London Police Service Desks is consistently very high and feedback from users achieved scores in excess of 90% each month. The Service Desks resolve over 75% of all calls and consistently ensure that calls are answered within target.
2. There were 2 P1 incidents in City of London which impacted internet access and Office 365 at London Councils. These were both caused by issues following security patching which required server restarts. Actions have been completed to ensure that there is no risk of repeat.
3. In June users in City of London were unable to send email outside of the organisation following a migration of the Office 365 platform. The incident report is being prepared by Agilisys and Microsoft but early indicators point to a Microsoft licensing issue which applied incorrect sending limits.
4. There were no P1 incidents in City of London Police.

IT Transformation Summary

5. Rollout of Office 365 will begin with the IT team in July followed by Comptroller's and Remembrancer's. This is subject to modifications with as a result of a current IT change freeze.
6. Of the 297 applications required, 60% of packaging is complete and a third of applications have passed User Acceptance Testing (UAT) and ready for Windows 10 deployment.
7. IT Business partners are working with Corporation departments on device selection with a mobile first policy.
8. Regular engagement across different Corporation sites to prepare colleagues for the desktop transformation and devices that will be available.
9. First 22 sites fully remediated including Guildhall.
10. Plan in place for remaining 90 sites to be complete by October 2017
11. LAN design, build and support tenders will be submitted by 19th July.

Police IT Programmes Update

12. Automatic Number Plate Recognition – It has been agreed that an ANPR work stream will be set up under the new Secure City Programme. There is a launch of the National ANPR Service on the 27th June 2017. Milestones delivered in this period include: Setting up the infrastructure and testing a secure PSN connection for the service.
13. Niche Programme (Note The NicheRMS™ Police Records Management System is an incident-centric tool that manages information in relation to the core policing entities: people, locations, vehicles, organizations, incidences and property/evidence). Milestones delivered in this period include: The Virgin Connectivity into Bishopsgate implemented; configuration and testing of

the desktops already in place for connectivity and access; roles and responsibilities, process mapping and SLA's will be completed during the next period.

14. Network Transformation - The Hardware supplier contract has been awarded and the programme is in the process of on-boarding. The GJR Exit Solution proposal has been approved and project delivery is underway. The outstanding Agilisys security clearances have now been received, and so remediation of CoLP sites can start.
    IMS-DRS (Integrated Management System and Driver Rectification System linked to the CCTV network) The segregated LAN has now been installed into Wood Street and is functioning. This will provide a Disaster Recovery Build to ensure in the event of a catastrophic failure of the IMS-DRS system, the Force Control Room at Wood Street will be provided with adequate IMS-DRS CCTV Station to support on-going operation.
15. Office 365 - Work is continuing on the preparation of the CoLP Office 365 business case. The time lines that individual police forces will be able to roll out Office 365 will be guided by the National Productivity Services Programme, led by the National Police Technology Council. Indications are that pilots will start in early 2018. In order to secure appropriate funds a business case will be presented in October /November 2017.

Risk Actions

16. Risk remains a key focus for the IT Division and we are continuing to ensure this drives the priority for project works and Change Management decisions. A Deep Dive exercise, Risk Workshop and the appointment of the IT Business Manager (who will own Division Risk) have moved the Corporation to a better position with regard to understanding its risk landscape and the on-going management of IT Risks.
17. Following further assessment, the IT Division currently holds 19 risks, of which 3 are RED. These risks are tracked in Covalent. All risks have actions, with target dates to enable tracking and management.
18. IT Corporate Risks that remain are:
    - CR16 IT Security - Update - 10 steps assessment has highlighted specific priority areas which are managing user privilege, remote access and user education and awareness. Delivery of Privilege Access Management solution begins to roll out throughout June and July)
    - CR19 IT Service provision - Update - expected to move to Amber by December 2017). For a summary of the status of these risks see Appendix A.

Memorandum of Understanding (MoU) between the IT Division and City Surveyor

19. A question was asked at the last IT Sub-Committee about the division of responsibilities for IT Data Communications rooms between Corporate IT and

Facilities Management. From a meeting held with the City Surveyor and Corporate IT since the last IT Sub Committee it was confirmed:

- The current state of the cabling supporting the IT infrastructure is a Corporate IT responsibility
- The remediation is the responsibility of IT and cost to resolve is within the Corporate IT budget
- All works will comply with relevant standards especially Health and Safety Standards
- IT will be responsible for all electrical cabling from the distribution board to the communications cabinet and all IT infrastructure cabling
- We will communicate on a site by site basis directly with the end users
- Corporate IT would provide advance notice to your Facilities Management of any works being undertaken
- Once fully remediated new processes will be enforced to ensure consistent good practice and management of IT assets and data communications rooms across the Corporation and City of London Police estate. The detailed MoU agreed is attached as Appendix B.

Corporate IT and Agilisys Contract Extension

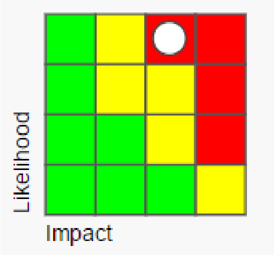
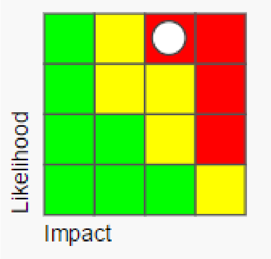
20. Preparation for contract negotiations with Agilisys for the extension of the existing IT contract has begun. The expectation is that negotiations will start in July 2017 and be completed by October 2017. A recommendations report regarding changes and improvements to the existing contract will be brought back to the IT Sub-Committee after this date.
21. A Workshop held with Members on 28th June 2017 to review the negotiation approach with Agilisys.
22. It is expected that the workshop will help officers understand Members' priorities regarding any enhancements to the contract and the extended richer Key Performance Indicators (KPI's).
23. The slides and any actions from this meeting will be circulated to Members as a late paper.

Sean Green
IT Director, IT Division
T: 020 7332 3430
E: sean.green@cityoflondon.gov.uk

Appendices

Appendix A – IT Corporate Risks Update
Appendix B – Memorandum of Understanding IT Division and City Surveyors

Appendix A: Update on IT-related Corporate Risks

Risk	Score	Heatmap	Latest update
CR16 – information Security	Likelihood: 4 (Likely) Impact: 4 (Major)		10 steps assessment has highlighted specific priority areas which are managing user privilege, remote access and User education and awareness. Delivery of Privilege Access Management solution begins to roll out throughout June and July; Secure reconfiguration of remote access solutions is underway; HR training lead working with CISO on user education and awareness campaign with a view to launch in July.
CR19 – IT Service Provision	Likelihood: 4 (Likely) Impact: 4 (Major)		The primary focus of the team is on stabilisation, a more robust approach to managing change has been adopted, reducing the risk of service interruption. Team level approach to risk management is now aligned fully to the top level approach. The risk is expected to reduce to Amber by December 2017 followed by steady progress to Green in the following months.

Appendix B – Memorandum of Understanding IT Division and City Surveyor

1 Purpose

The purpose of this Memorandum of Understanding (MoU) between the IT Division and City Surveyors is to define the standards required for IT Communications (Comms) rooms in the future, ownership of the Communications rooms and the split of responsibilities between the IT Division and the City Surveyors department.

2 Communications (Comms) Room Standards

2.1 Hosted Equipment

It is agreed the all Comms rooms hosting IT equipment are the responsibility and are under the ownership and supervision of the IT Division (IT Director or a delegated member of the IT team). No changes in these rooms or access provided (outside emergencies) can be made without the agreement of the IT Division.

A Comms Room will typically host the following hardware:

- Active network equipment
- UPS
- Cabinets
- Patch panels
- Servers. (NB. There should be no Servers on remote sites, but there are currently 10 on remote sites which will be required until they can be safely decommissioned.)
- Air conditioning

Comms Rooms must be tidy and there must be no old equipment, boxes, cabling or other items on the floor.

2.2 Location & Other Building Services

The location of the Comms Room shall comply with the requirements specified below and where any retrospective changes are required it is the IT Division responsibility to seek appropriate funds and oversee the works

2.2.1 The Comms Room must not be located adjacent to fixed spaces such as lift shafts or toilet blocks;

2.2.2 To maintain the integrity of the Comms Room the room should be designed and constructed to resist water ingress, there must be no risk of flooding the Comms Room from sprinkler systems within the rooms or elsewhere in the building. A doorsill should be provided where needed.

2.2.3 Building services not supplying the Comms Room itself will not run through it. Ideally this would also apply such that they are not directly beside, above or below it but where this cannot be avoided the building services shall be installed in a manner such that in the event of a leak it will not cause direct damage to the server equipment. The services that this includes:

- Water mains, water storage, supply/waste pipes and drainage
- Gas mains
- Electrical supplies (not relating to the Comms Room)
- Air Conditioning Services (not relating to the Comms Room)
- Sewage pipe work
- Sprinklers should not be provided in the Comms Room.

2.3 Physical Requirements

2.3.1 Minimum height of the rooms should be 2.6m from the finished floor to any overhead obstructions or ceiling **and where any retrospective changes are required it is the IT Division responsibility to seek appropriate funds, identify a new location and oversee the works**

2.3.2 The floor construction should be suitable for heavy Server, Telecommunications and Power Supply Systems, the floor should able to support up to 6 cabinets each weighing up to 500Kgs;

2.3.3 The main and intermediate door[s] leading from the circulation space, through to the Server or Hub Rooms shall be a minimum of 900mm wide and 2130mm high, with doorsills to be provided where required to prevent adjacent sprinkler water entering the Comms Room, hinged to open outwards (building regulations permitting).

2.3.4 The door[s] shall be secured by the building access control system. Where this is not possible, a combination security locking mechanism such as Digi locks should be used;

2.3.5 The entrance to the Comms Room should be finished floor level except for the doorsill where provided to prevent water ingress;

2.3.6 Room decor – finished in light, easy to clean non static finish.

2.4 Power in Comms Rooms Standards

2.4.1 Clean circuits must be designed to minimise the possibility of a trip in another part of the building affecting the power supply to the Comms Room;

2.4.2 Cable routing must be provided so that electrical cables are not trailing on the floor and do not obstruct full access to the rear of the racks;

2.5 Earthing Standards

2.5.1 Earthing is to be provided on a dedicated earth bar to current building standards. The IT infrastructure maintenance provider is responsible for ensuring all equipment including the cabinets is earthed correctly to standards detailed below:

2.5.2 BS6701 – Telecommunication cabling and equipment installations;

2.5.3 BS7671 – Requirements for electrical installations: IEEE wiring regulations.

2.6 Communications (Comms) Room Environmental Standards

The Comms Room will be designed and constructed to meet the following environmental specifications and where any retrospective changes are required it is the IT Division responsibility to seek appropriate funds and oversee the works:

- Dry Bulb Temperature: 20°C to 28°C;
- Max temperature rate of change: 5°C per hour;
- Humidity levels as achieved by well-maintained air conditioning systems;
- Windows should not be provided in the Comms Rooms, where this is unavoidable, windows should be secured with security grills or bars;

- Air cooling by way of air conditioning or other acceptable mechanical means must be provided. The room heat load will be calculated using equipment lists and / or the CIBSE guidelines;

2.7 Comms Room Additional Standards

2.7.1 Physical Standards

2.7.1.1 The Comms Room must have minimum internal dimensions between finished walls of 6500mm x 3500mm **and where any retrospective changes are required it is the IT Division responsibility to seek appropriate funds and oversee the works**;

2.7.1.2 The walls should be of suitable construction for heavy Mechanical servicing systems (the type that ordinarily would be expected to be found in a Comms Room) to be wall mounted;

2.7.1.3 Lighting shall be a minimum of 300 lux in the horizontal plane and 150 lux in the vertical plane, measured 1000mm above the finished floor.

2.7.2 Power Standards

The following requirements apply unless there is a bespoke need to exceed them due to the nature of the equipment being housed in the Comms Room and where any retrospective changes are required it is the IT Division responsibility to seek appropriate funds and oversee the works:

2.7.2.1 Dedicated Comms Room 3 phase Distribution Board with internal stop switch located within Comms Room;

2.7.2.2 Up to 7kVA total power requirement for each Cabinet;

2.7.2.3 Each cabinet will be provided with a resilient pair of dedicated 32 amp, 230 volt three phase, clean supplies through an IEC 60309 connector;

2.7.2.4 A minimum of 12 x 230V13A sockets as per the Environmental Schedule are required within the Comms Room for use with non-Server related power requirements (i.e. technician’s laptop or test equipment). The final position of these outlets will be determined by the design and consultation process;

2.7.3 Heat Gain Standards

The table below provides the indicative heat output required for the cooling / air conditioning design. Final configuration may vary but output figure will remain. Note that these figures are for a single rack and do not include additional output that may be required to allow for other thermal gains and support any other systems required by the construction, M&E or FM provider, such as additional devices to run control software or additional PoE switches to power BMS or access control points. Exact cooling requirement in each Comms Room may vary.

Description	Thermal (Watts)	BTUs/Hr
Typical Network Rack	3625	8334

Comms Room Heat Gain

2.7.4 Environmental Standards

The Comms Room will be designed and constructed to meet the additional environmental specifications:

2.7.4.1 Humidity levels as achieved by well-maintained air conditioning systems;

2.7.4.2 DX Air Conditioning Units installed (N+1 Configuration) the position of which shall be agreed;

A gas suppression fire extinguishing system is required to be installed in the Comms Room; this should be capable of being activated from outside the Comms Room.

2.7.5 Environmental Sensors

An environmental sensor will be installed in each Comms Room by the IT infrastructure maintenance supplier. The sensor should have the following characteristics:

- Rack mountable
- RJ45 port(s) for Ethernet connection
- DHCP support for IP address assignment
- Remotely configurable using secure protocols such as HTTPS and/or SSH
- Role-based access control (e.g. view, control, administer)
- Temperature monitoring

- Remote temperature sensors for monitoring multiple cabinets in a single comms room. There should be a temperature sensor in every rack.
- Humidity monitoring
- Multi-level information, warning, and alarm generation.
- Full SNMP management information base (MIB) for monitoring and alarm trap generation
- Email alarm generation (SMTP/POP support)
- SMS alarm capability
- Ability to export logs and debugging information to a Syslog server
- Built-in display
- Accurate internal clock with power backup
- Expansion ports for additional sensors and web cams

Optionally, it is desirable for the environmental monitors to support additional features such as the following:

- Centrally-installed, dedicated software for the management of all sensors.
- Air flow monitoring
- ‘Dew point’ monitoring
- Water sensor
- Water leak rope
- Smoke detection and alarm
- Power failure detection and alarm
- Sound monitor
- Light level monitor
- Cabinet door sensor
- Audible alarm
- Analog ports

2.7.6 Split of Responsibilities between the IT Division and City Surveyors

- The current state of the cabling supporting the IT infrastructure is a Corporate IT responsibility

- The remediation is the responsibility of IT and cost to resolve is within the Corporate IT budget
- All works will comply with relevant standards especially Health and Safety Standards
- IT will be responsible for all electrical cabling from the distribution board to the communications cabinet and all IT infrastructure cabling
- We will communicate on a site by site basis directly with the end users
- Corporate IT would provide advance notice to the Facilities Management of any works
- Once fully remediated new processes will be enforced to ensure consistent good practice and management of IT assets and data communications rooms across the Corporation and City of London Police estate
- Any facilities changes that impact IT will be communicated to the IT Change process
- IT own and are responsible for any equipment that are in IT communications rooms
- IT are responsible for agreeing access to all IT communications rooms

Agreed By:

_________________________Date:
(Paul Wilkinson - City Surveyor)

_________________________Date:
(Sean Green – IT Director

Committees:		**Dates:**
Choose an item. Projects Sub Committee IT Sub Committee		18 July 2017 14 July 2017
Subject: Council Tax & Business Rates	**Gateway 7 Outcome Report Light**	**Public**
Report of: Chamberlain **Report Author:** Kevin Mulcahy, Head of IT –Projects & Programmes		**For Decision**

Summary

• Capital Project Number	81 1000 9
• Project Status Compared to GW2	Budget : Green Specification: Green Programme: Green
• Project Status Compared to GW5	Budget: Green Specification: Green Programme: Green
• Project status	Green
• Timetable	Close the Council Tax & Business Rates project (July 2017). The project is complete pending approval of this report (July 2017).
• Total Estimated Cost @ Gateway 5	£628,000
• Final spend at completion	£562,144.21 (Closed in Oracle in March 2015).
• Overall project risk	Green

Recommendations

1. It is recommended that the project be closed.

Main Report

1. Brief description of project	Council Tax and Business Rates teams are being TUPE'd back to the City of London by the 3rd October 2014 from the current service provider, Liberata. This involves the relocation of about 30 staff moving into the 2nd floor Walbrook Wharf office. Also, additional modules (e.g. self service portal and mobile) were being implemented. NB Due to legacy issues, this project was never formally closed. This report is to seek closure and accordingly, some detail may be missing.

2. Assessment of project against SMART Objectives	The project delivered the required infrastructure to allow the 30 staff members to work in Walbrook Wharf. P1 – Core Models – Live 31/07/12 P2 – Self Service – Live 24/06/13 P3 –Live Billing – Live 06/10/14
3. Assessment of project against success criteria	1. All staff working in new location
4. Key Benefits	**1.** DR location moved and now more resilient. **2.** Continuation of service
5. Was the project specification fully delivered (as agreed at Gateway 5 or any subsequent Issue report)	Yes
6. Programme	The project was completed within the agreed programme
7. Budget	The project was completed within the agreed budget
Final Account Verification	Verified Please confirm whether or not the Final Account for this project has been verified. * State any outstanding issues, actions to be taken and timescales for resolution. There are no outstanding financial issues.

Review of Team Performance

8. Key strengths	**1.** Core functionality returned in house
9. Areas for improvement	**1.** Multi phase project could have been more focused with tighter delivery team and shorter timescales

	2. Complete close down activity sooner
10. Special recognition	**1.** N/A

Lessons Learnt

11. Key lessons	**1.** More focused with tighter delivery team and shorter timescales
12. Implementation plan for lessons learnt	**1.** Projects should engage with all key personnel early and confirm requirements

Contact

Report Author	Kevin Mulcahy
Email Address	Kevin.mulcahy@cityoflondon.gov.uk
Telephone Number	0207 332 3428

This page is intentionally left blank

Agenda Item 7

Committee(s)	**Dated:**
IT Sub Committee – For Information	14 July 2017
Subject: GDPR Briefing	**Public**
Report of: The Chamberlain	**For Information**
Report authors: Sean Green & Gary Brailsford-Hart	

Summary

- The purpose of this report is to brief Members on the General Data Protection Regulations (GDPR) that will replace the Data Protection Action 1998, coming into force in May 2018.

- This report provides a brief overview of GDPR and additional or changed responsibilities from the current required DPA compliance responsibilities.

- The report also outlines next steps to ensure both the Corporation and City of London Police are compliant with GDPR.

Recommendation(s)

Members are asked to:

- *Note the report.*

Main Report

Updates

General Data Protection Regulations

1. GDPR is the new EU regulation that comes fully into force on 25th May 2018. The regulations introduce uniform rules for data protection across Europe. The regulations are intended to make data regulation fit for the digital world we now live in. From the 25th May 2018, the regulations will replace the Data Protection Act (DPA) (1998).

2. The core principles of current Data Protection legislation remain unchanged. However the GDPR adds new obligations to provide a higher level of protection of personal data and these new obligations could require additional effort in order to comply with and meet these requirements. The Corporation has an Information Management Board chaired by Michael Cougher the Senior Information Responsible Officer (SIRO) for the Corporation and the City of London Police also has an Information Management Board chaired by their SIRO, the Commissioner.

3. The purpose of GDPR is to protect the privacy of individuals; ensure that data is not processed without the knowledge and consent of individuals; to grant data subjects various additional rights (including greater scope their rights to access their data).

4. The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

5. Current DPA states the following eight principles:

   - Data shall be processed lawfully
   - Data shall be processed for a specified purpose
   - Data shall be adequate, relevant and not excessive
   - Data shall be accurate and up to date
   - Data shall not be kept longer than necessary
   - Data shall be processed in accordance with the rights of data subjects
   - Data shall be kept secure
   - Data shall not be transferred outside of the European Economic Area (EEA) with adequate controls

6. In summary compared to the DPA, GDPR will result in:

   - More data being in scope;
   - Corporation Suppliers and processors of data in scope;
   - Tougher sanctions for breaches;
   - Compulsory notifications to the Information Commissioner of data breaches;
   - More rights for individuals;
   - Explicit recording and management of consent;
   - A new statutory senior role for the Data Protection Officer;
   - Greater accountability and governance.
     (Note: Appendix A provides a more detailed breakdown of the changes)

7. Within the Queens Speech of 21st June the Data Protection Bill was confirmed. The Government has stated that the new UK bill would ensure the country met its obligations while a member of the EU, and would help the UK maintain its "ability to share data with other EU member states

and internationally after we leave the EU". The new bill will replace the Data Protection Act 1998. The government has stated its key priorities as follows:

- ensuring data protection rules were "suitable for the digital age";
- "empowering individuals to have more control over their personal data";
- giving people the "right to be forgotten" when they no longer wanted a company to process their data - providing there were no legitimate grounds for a company retaining the data;
- modernising data processing procedures for law enforcement agencies;
- allowing police and the authorities to "continue to exchange information quickly and easily with international partners" to fight terrorism and other serious crimes.

8. An audit is being commissioned with internal audit to help the Corporation identify gaps in compliance and then produce an action plan (possibly requiring a project) to address these gaps. The GDPR audit includes:

- readiness assessments, detailed risk-based compliance assessments across all GDPR clauses and themed compliance reviews e.g. cross-border transfer analysis, implementation of our compliance program and on-going monitoring;
- Privacy Impact Assessments (PIA);
- breach response reviews;
- third-party privacy reviews;
- design and implementation of privacy and operating models;
- data protection internal audits;
- training and awareness programmes;
- audit compliance, implementation and change management related to GDPR; and
- cyber security and information security.

9. It should be anticipated that the new GDPR regulations will require new or updated policies, procedures and possible changes to employee roles and guidance as well as additional technical enablers to manage the tracking of assets and consent. This will need to be backed up by new training materials, communication and awareness.

10. Based on the findings from the audit and the 12 steps preparation guidelines issued by the Information Commissioner's Office (ICO) see Appendix B, Director of Information will finalise the action plan across the Corporation and the City of London Police.

11. A further update on GDPR will be brought back to the IT Sub-Committee in November 2018.

Sean Green
IT Director
T: 020 7332 3430
E: sean.green@cityoflondon.gov.uk

Gary Brailsford-Hart
Director of Information
T: 020 7601 2352
E: Gary.Brailsford@cityoflondon.pnn.police.uk

Appendix A – DPA Obligations comparison with GDPR

Theme	DPA	GDPR
Rights of Data Subjects	• Access to personal data • Prevent processing likely to cause damage or distress • Prevent processing for direct marketing • Object to automated decision making • Have inaccurate personal data removed • Claim compensation for damages caused by a DPA breach	• Data portability • To be forgotten • Object to processing
Subject Access Requests	• Where an individual requests access to their own information • Required ID and a written request • 40 day deadline to respond • £10 fee required	• Deadline to respond 1 month • No fee required
Data Breaches	• Report to Senior Responsible Information Officer (SIRO) • No need to report to the Information Commissioner's Office (ICO) • Maximum fine £500,000	• Must be reported to ICO within 72 hours • Fines up to 2% of turnover or €10m for poor record keeping, contracting etc • Fines of up to 4% of turnover or €20m for breaches of rights or principles • New definition 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, transmitted, stored or otherwise processed
Privacy Notices and Consent	• A privacy notice should contain: The identity of the data controller; the purpose for which you intend to process the information; any extra information you need to give individuals the context to enable you to process the information fairly • Soft opt in to data protection and use of information for specified reasons is permitted (e.g. tick this box if you don't want us to use your information)	• Show the legal basis for processing information • Data must be trackable • No more 'soft opt ins' • Controller must prove consent
Privacy Impact Assessments	• Not Mandatory • Recommended when processing large amounts of data	• Mandatory for all business cases • Privacy by design
Other Considerations		• DPA Officers mandatory role in an organisation processing data • Consent for use of Children's Data • Child likely to be defined as anyone under 13 years of age

Appendix B – Information Commissioners Office: 12 steps preparation guidelines

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now

1 Awareness You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 Consent You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8 Children You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11 Data Protection Officers You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Introduction

This checklist highlights 12 steps you can take now to prepare for the General Data Protection Regulation (GDPR) which will apply from 25 May 2018.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

It is important to use this checklist and other Information Commissioner's Office (ICO) resources to work out the main differences between the current law and the GDPR. The ICO is producing new guidance and other tools to assist you, as well as contributing to guidance that the Article 29 Working Party is producing at the European level. These are all available via the ICO's Overview of the General Data Protection Regulation. The ICO is also working closely with trade associations and bodies representing the various sectors – you should also work closely with these bodies to share knowledge about implementation in your sector.

It is essential to plan your approach to GDPR compliance now and to gain 'buy in' from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR's new transparency and individuals' rights provisions. In a large or complex business this could have significant budgetary, IT, personnel, governance and communications implications.

The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas listed in this document will require organisations to review their approach to governance and how they manage data protection as a corporate issue. One aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organisations.

Some parts of the GDPR will have more of an impact on some organisations than on others (for example, the provisions relating to profiling or children's data), so it would be useful to map out which parts of the GDPR will have the greatest impact on your business model and give those areas due prominence in your planning process.

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one.

Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas.

The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and those individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

The ICO's Privacy notices code of practice reflects the new requirements of the GDPR.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;

- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new. It only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine readable form and provide the information free of charge.

5 Subject access requests

You should update your procedures and plan how you will handle requests to take account of the new rules:

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

6 Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to help you comply with the GDPR's 'accountability' requirements.

7 Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

You should read the detailed guidance the ICO has published on consent under the GDPR, and use our consent checklist to review your practices. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data.

You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

8 Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'.

This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

10 Data Protection by Design and Data Protection Impact Assessments

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

You should also familiarise yourself now with the guidance the ICO has produced on PIAs as well as guidance from the Article 29 Working Party, and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

- a public authority (except for courts acting in their judicial capacity);
- an organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
- an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions. The Article 29 Working Party has produced guidance for organisations on the designation, position and tasks of DPOs.

It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

12 International

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this.

The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.

This is only relevant where you carry out cross-border processing – ie you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states. If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

The Article 29 Working party has produced guidance on identifying a controller or processor's lead supervisory authority.

Committee(s)	Dated:
IT Sub – For Information PRED Sub – For Information	14 July 2017 21 September 2017
Subject: Website Update and Action Plan including Memorandum of Understanding between the IT Division and Communications Division	**Public**
Report of: Director of Communications and IT Director	**For Information**
Report author: Director of Communications Bob Roberts and IT Director Sean Green	

Summary

At the May meeting of the IT Sub Committee Members expressed concern at the oversight of the website and asked for an outline of the service responsibilities shared by the Director of Communications and IT Director for the website and the intranet.

The document detailing responsibilities is attached at Annex A.

However both the IT Director and the Director of Communications also wanted to take the opportunity to update members on the actions taken and being planned to improve the website.

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. Responsibility for the management of the Publishing Team which includes staff running the City Corporation's website and intranet was given to the Director of Communications from the retiring Deputy Town Clerk on October 1st 2016.

Current Position

2. A short review found there was widespread dissatisfaction with the website launched in 2012 which is now showing its age.

3. A number of actions have already been taken and more are planned. They are:

    - A new editorial policy was introduced in March 2017 to ensure there was strong editorial governance to improve the experience of people who use our websites and digital platforms and allow us to use plain English as standard.
    - In March 2017 consultants were appointed to advise on the state of the website and how to improve user experience. The consultants are expected to report at the end of June.
    - In June 2017 a new policy was introduced detailing permissions needed if City of London Corporation institutions wanted to set up their own website separate from the City Corporation website to end the confusion about when standalone websites were allowed.
    - In September 2017 the IT and website teams plan to reintroduce a default 12 month expiry system to ensure all pages – and the metadata which optimises search results – are reviewed once a year or are removed from the website. This would be backed up by a message from the Director of Communications to ensure web page editors must update pages.
    - In September 2017 we will review the 100 most-popular pages of content to ensure all information and metadata is up to date. Already, the top 250 pages are tested every week for function/links, email links, accessibility, code quality, SEO and metadata, performance and spelling.

4. Members should also be aware that the system which is used to manage the content of our website (Sharepoint) will not be supported by Microsoft from 2020. A new content management system will have to be found. This has implications for both the Member section of the website and the search engine which both still cause concern for Members and users.

5. On Member content, this is hosted by a third-party site. If Members wished to incorporate this information in a new section on our website we should be aware this would be an expensive (circa £100,000), major project and also against agreed IT policy that we should not duplicate functions provided by other sites. It would also only be a solution until 2020 when our content management system will have to be changed.

6. On the search engine and its functionality it is recognised this remains an issue and performs badly compared to Google search. However Google Search cannot be installed on our own website as it would mean allowing Google access to our systems posing a security risk. A new search system could be designed and installed however this would be an expensive option again bearing in mind it would only last until 2020. If Members wished the search function could be removed.

7. A report on future options for the website will be brought to Members after the consultants have completed their report. It is expected to examine whether it is cost-effective or necessary to start the process of redesigning or relaunching the website bearing in mind the need for efficiency savings and other priorities of the City of London Corporation.

Conclusion

Members note the Action Plan and the outline of the service responsibilities shared by the Director of Communications and IT Director

Appendices

1. Outline of the service responsibilities shared by the Director of Communications and IT Director

Bob Roberts and Sean Green
Director of Communications and IT Director

T: 020 7332 1111   T: 020 7332 3430
E: bob.roberts@cityoflondon.gov.uk   E: sean.green@cityoflondon.gov.uk

Appendix A Outline of the service responsibilities shared by the Director of Communications and IT Director

1 Purpose

The purpose of this Memorandum of Understanding (MoU) between the IT Division and Communications Team is to define the standards required for support and management of the corporate website including the split of responsibilities between the IT Division

2 Roles and Responsibilities

2.1 Communications Team

The Communications Team are responsible for content on the main website, e.g. text, images, PDFs. This excludes: Member content; Jobs; transactions, (i.e. report, pay, apply forms; online shop and GIS mapping). News releases are updated separately by the Media Office.

The Communications Team also manage website statistics using Google Analytics. Additionally, they also have responsibility to ensure that content is accessibility compliant, that plain English is used throughout and that the focus is on the user.

The Director of Communications has overall responsibility for the content and design of all the City Corporation’s websites and digital platforms.

The Communications Team should oversee and regulate all digital output as the office has ultimate responsibility for all communication originating from the City Corporation. This covers all digital assets including the intranet, apps and social media.

2.2 IT Technical Web Team

The technical support staff supporting the corporate website are from the Agilisys Shared SharePoint services team. This team comprises of SharePoint Administrators, Developers and Architects.

SQL Data Base Administration support is provided by the Agilisys Shared Database Services Team. Infrastructure support is provided by the Agilisys Infrastructure services.

Application Support & Maintenance	Corporate IT
1. Investigating SharePoint software issues reported to the Service Desk and liaising with Microsoft where necessary for resolution.	X
2. Installing cumulative updates and Service Packs for SharePoint solutions and 3rd party software on SharePoint Servers when required	X

Application Support & Maintenance	**Corporate IT**
3. Carrying out bug fixes across agreed SharePoint solutions as per agreed incident priorities and SLAs in Schedule 2.2	**X**

Application Administration	**Corporate IT**
1. Administration of SharePoint service applications	**X**
2. Performing Service Request & Change Management	**X**
3. Performing Incident and Problem Management in alignment with Schedule 2.1	**X**
4. Conducting troubleshooting, technical investigations and root cause analysis into defects/ performance issues with SharePoint solutions	**X**
5. Undertaking the following monitoring activities • Conducting weekly SharePoint log monitoring • Regular monitoring of application availability • Management of application storage • SharePoint database status monitoring • Search crawl log monitoring Timer Job status monitoring	**X**

Application Development and Management	**Corporate IT**
1. Technical management of SharePoint sites across SharePoint instances	**X**
2. Management of SharePoint services on servers/ Office 365 tenancies	**X**

3. Managing SharePoint Server Farm features	X
4. Understanding and documenting application architecture and functionality for SharePoint solutions	X
5. Supporting enforcement of established SharePoint governance	X
6. Supporting the development of SharePoint roadmaps which align to organisational goals and business priorities	X
7. Developing BAU feature enhancements for existing SharePoint solutions. Note. If required, enhancements over 5 days of effort will be a project in accordance with clause 11.	X
8. Supporting the continued rationalisation of SharePoint platforms to ensure standardisation and optimising supportability Note. Subject to requirement, rationalisation work will be a project in accordance with clause 11.	X
9. Designing SharePoint solutions based on established patterns and best practices focusing on User Adoption and Governance	X
10. Management and maintenance of development roadmaps across all SharePoint solutions, including documentation of requirements, bug fixes and feature requests	X
11. Providing SharePoint technical development support capability across all versions of SharePoint including C#, PowerShell, HTML, CSS, jQuery, CSOM	X
12. Provision of consultancy, advice and guidance during the build-up to one major migration of each SharePoint instance, up to a maximum of 5 days per instance.	X

3 Service Levels Applicable

3.1 Communications Team

- Submitted content should be approved within 24 hours.
- Content will be updated at least every 12 months by content owners

IT Technical Web Team

The SLA's align to the normal contractual SLA's reported monthly to IT Sub-Committee Members.

- Priority 1 incidents resolved in 2 hours
- Priority 2 incidents resolved in 6 hours
- Priority 3 incidents resolved in 8 hours

Agreed By:

__________________________Date:
(Bob Roberts – Director of
Communications)

__________________________Date:
(Sean Green – IT Director)

This page is intentionally left blank

Agenda Item 9

Committee(s)	**Dated:**
IT Sub Committee – For Information	14 July 2017
Subject: Open Mediated Wifi provision for Guildhall Events	**Public**
Report of: The Chamberlain	**For Information**
Report author: Matt Gosden, Deputy IT Director	

NOT FOR PUBLICATION

By virtue of paragraph [insert exemption clause as per separate guidance] of Part 1 of Schedule 12A of the Local Government Act 1972

Summary

Provided by O2 and procured through G-Cloud, Open Mediated Wifi ("OMW") was deployed across four main sites in December 2015 to provide Wireless internet connectivity for members and guests of the Corporation. With a further three sites provided with this service in 2016/17.

- This was designed to be a free, unrestricted Wifi service, separate from the Corporate wired and wireless network. Providing sufficient bandwidth and capacity for basic internet connectivity, much like guest Wifi available in a coffee shop.

- As a registration-free, free-to-use service, the provision has been largely stable, however additional business requirements have been identified since the project was delivered and closed.

- Some of these requirements have been addressed in service improvement measures taken to date, detailed further in the report.

- The remaining business requirements will be included in the new generation of OMW, which will be procured to coincide with the contract expiry in December 2017, subject to approval and additional funding where required:

    1. High Density, high bandwidth internet connectivity, with an extended hours support wrap and improved Service Level Agreement for the Events team, designed around requirements from the Remembrancers to allow the Corporation to continue to compete in the Conferencing and Events market;

    2. Deployment to other Corporation sites, including New Street Police Station, HARC and the Markets.

This paper details the current situation with Open Mediated Wifi (OMW), the provision for the Events team and additional improvements made; and the proposed next steps for the next generation of OMW (“OMW2”.)

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. Public Open Mediated WiFI (OMW) was implemented in December 2015, procured through GCloud.

2. The business requirement for this service was to provide basic, free unrestricted guest wifi, separate from the corporate wired and wireless networks. Initially across four key Guildhall sites:

    - Guildhall
    - Walbrook Wharf
    - Bishopsgate
    - Mansion House

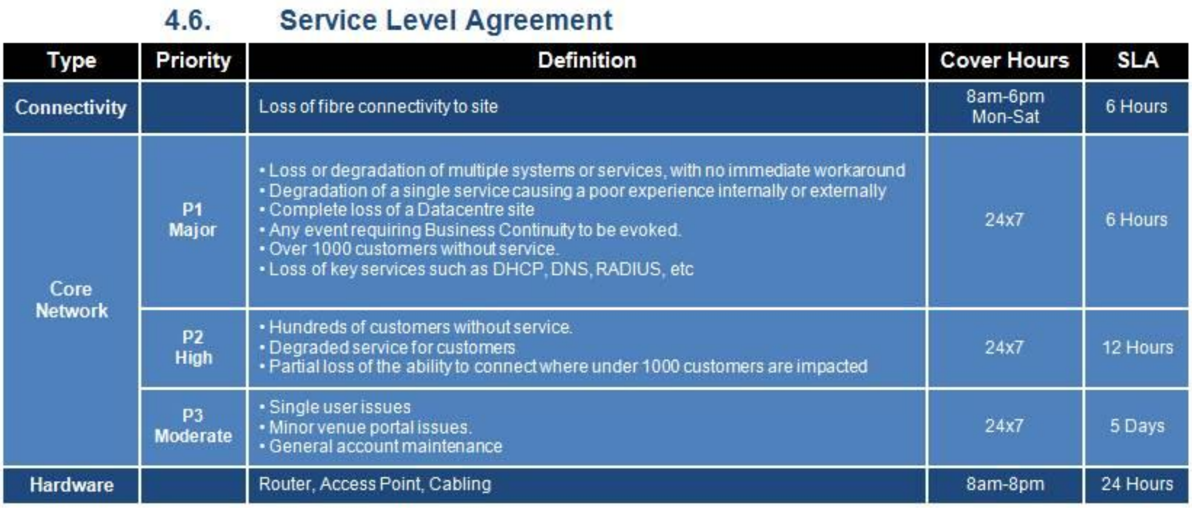
    And then later, in 2016/17 it was implemented in:

    - London Metropolitan Archive
    - Lauderdale Housing Office
    - Tower Bridge

Current Position

3. Whilst the service has proved to be broadly stable across COL sites, it was designed and implemented for infrequent, low-density use by occasional guests (much like the free wifi available in a coffee shop.)

4. In keeping with the level of service the OMW was designed to provide, the contract with O2 provides support between 08:00-18:00, with a comparatively slow SLA response in the event of an incident:



4.6. Service Level Agreement

Type	Priority	Definition	Cover Hours	SLA
Connectivity		Loss of fibre connectivity to site	8am-6pm Mon-Sat	6 Hours
Core Network	P1 Major	• Loss or degradation of multiple systems or services, with no immediate workaround • Degradation of a single service causing a poor experience internally or externally • Complete loss of a Datacentre site • Any event requiring Business Continuity to be evoked. • Over 1000 customers without service. • Loss of key services such as DHCP, DNS, RADIUS, etc	24x7	6 Hours
	P2 High	• Hundreds of customers without service. • Degraded service for customers • Partial loss of the ability to connect where under 1000 customers are impacted	24x7	12 Hours
	P3 Moderate	• Single user issues • Minor venue portal issues. • General account maintenance	24x7	5 Days
Hardware		Router, Access Point, Cabling	8am-8pm	24 Hours

5. Feedback from the Remembrancer’s Team has showed that OMW and the supporting contract and SLA does not provide the density or bandwidth required for large, heavily populated events in the Great Hall, Livery Hall, Old Library, Crypt and other areas, where demand for high capacity services such as media streaming or interaction between attendees with high numbers of connected devices is becoming more commonplace. In addition, there have been reliabililty issues within events areas, causing significant problems for the Remembrancer’s team and their customers. As many events occur outside the contracted support hours, this has also caused additional issues with supporting the service when issues occur.

6. The OMW capability in the Events areas provides the following capacity and connections:

	Approx Number of Concurrent Users	Number of "Hardwired" Connections Available
Great Hall	300	6
Old Library	150	4
Livery Hall	150	4
Crypts	150	4 (in each crypt)
Print Room	80	2
Basinghall Suite	80	2
Basinghall Street Entrance	80	0
Ambulatory o/s Great Hall	80	0

The City of London Corporation Open Mediated WiFi is delivered over a 1GB dedicated circuit.

7. Although the project is formally closed, the IT Project Manager, the Head of VIP Services (acting as Business Partner for Remembrancers) and Deputy IT

Director have worked with Remembrancers and O2 to improve the service within the scope of the current contract.

Steps taken include:

- Surveys to widen the scope of the OMW service to other COL sites, including weeding the wifi names (SSIDs). By configuring each site to only broadcast the SSIDs relevant to it, unneccesary traffic was reduced, improving connectivity and reliability.
- Working closely with O2 to ensure that all the O2 managed equipment is monitored appropriately, allowing IT to respond to incidents quickly and analyse connectivity and usage data more effectively to measure the demand.
- Following an in-depth survey by O2, IT re-sited some of the Access Points in events areas. Access points broadcast their signal in a specific direction. By re-siting some of these, IT were able to improve the coverage and signal strength in areas where obstacles were previously causing issues, such as stone pillars or thick doors.
- The Deputy IT Director identified as the Service Owner, to ensure open communication with customers and focus on improving the existing service and preparing for the next generation of OMW.
- In the Great Hall and other high density areas, IT have provided dedicated, wired internet access to reduce the impact on the wifi service and provide higher capacity and bandwidth for the event host's presentations.
- Where high profile events call for additional support, O2 have provided additional monitoring and remote and on-site support.
- O2 performed a survey to scope and price a High Density Wifi solution for events areas. The budgetary costs for this proposal would be £155,000 capital and an increase of £554 revenue per month to £2,454.

Next steps

8. The current OMW contract was procured through G-Cloud, the O2 contact expires after a 24 month term in December 2017.

9. Working with Procurement and Remembrancers, the IT Team are producing the requirements to procure a provider for the next stage of OMW with a proposed 3 year contract.

10. City of London Corporation owns the hardware, reducing the complexity of the transition to the new contract, however, additional requirements will be built into the new proposed solution for procurement, including:

    - High Density wifi in events areas: This is a different class of solution to meet demand in these areas. Providing improved capability for a high density, high bandwidth service to better meet the need of our customers and compete in the events and conferencing market.

- OMW deployed to a further 26 COL and COLP sites, including Tilbury BIP, HARC, New Street Police Station, Monument, Smithfield, Billingsgate and Spitalfields markets.
- Improved support, with increased support hours and improved SLA where required.

11. The new OMW solution will operate alongside the secure Corporate WiFI, delivered through Network Transformation and the City wide 1gigabit public Wifi currently being provisioned by Open Spaces.

12. The Outline documentation for this procurement has been submitted to the IT Project Management Office to commence the process of scoping and costing the new solution and navigating the governance boards for the increase in funding.

Matt Gosden
Deputy IT Director
E: matt.gosden@cityoflondon.gov.uk T: 0771 474 6996

This page is intentionally left blank

Information Technology Sub-Committee - Work Programme

September 2017

- LAN Services and Support Award **- Strategic**
- Information Management Briefing- **Strategic**
- IT Finance Update & early view of 2018/19 Budget - **Operational**
- Unified Communications and New Telephony Business Case – **Strategic**

November 2017

- 2018/19 Budget Review Update - **Operational**
- Agilisys Contract extension recommendations - **Strategic**
- Members Survey and Action Plan - **Operational Improvement**
- Digital and Applications Strategy Design Principles - **Strategic**

Further Ahead

- Ways of Working Pilot Review - **Strategic**
- End of Agilisys Contract Transition Planning - **Strategic**
- Information Management Review **- Strategic**
- Applications Rationalisation Review - **Strategic**

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Agenda Item 15

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Agenda Item 16

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Agenda Item 17

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Agenda Item 18

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Agenda Item 19

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Agenda Item 20

Document is Restricted

This page is intentionally left blank

Agenda Item 21

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

Agenda Item 22

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

Agenda Item 23

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Agenda Item 25

Document is Restricted

This page is intentionally left blank

Agenda Item 26

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank