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:

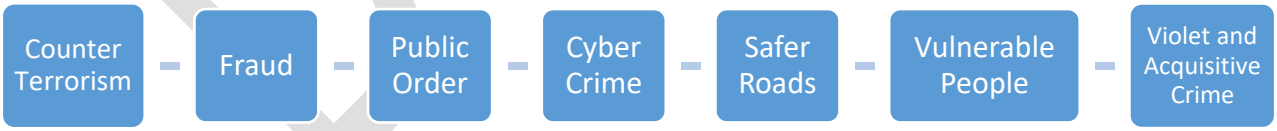


Figure 1 – Policing Priorities – City of London Policing Plan 2017

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

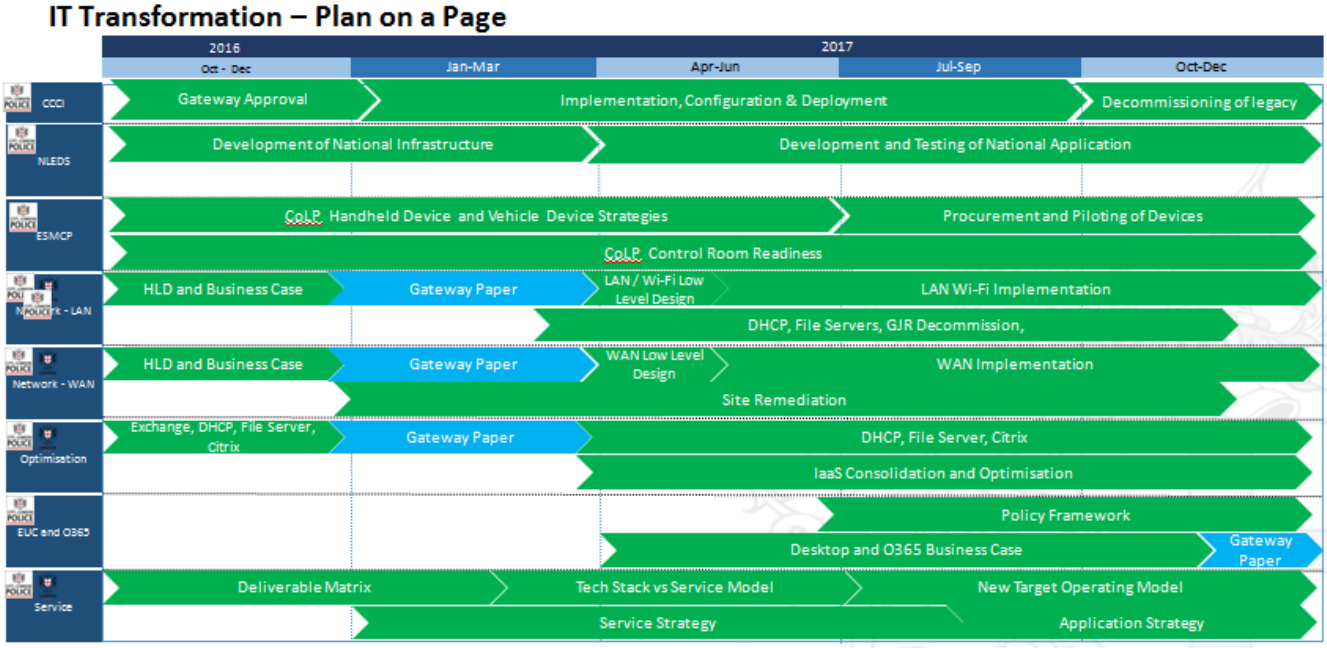
We will seek to align the applications and infrastructure roads maps that we deliver, with the requirements of national change programmes across policing. We will provide the appropriate levels of horizon scanning to ensure that there is a detailed understanding of what programmes such as The Home Office 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

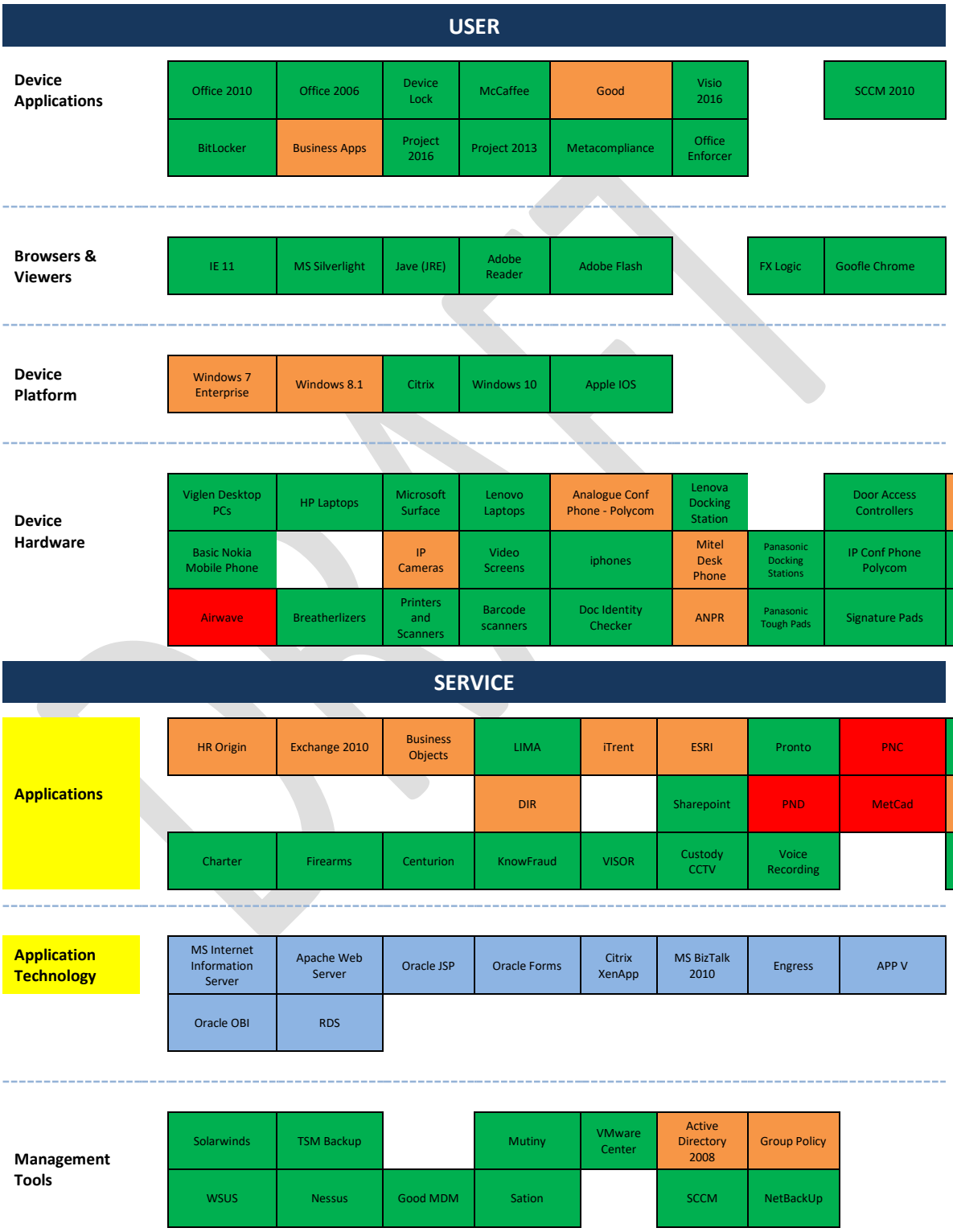
- Minimise business impact
- Reduce the impact of rework and change
- Sequence the changes to deliver maximum user benefit
- Follow good industry practice
- Understand the interdependencies with other programmes such as ring of Steele and Accommodation Programme
- Be clear on readiness criteria and enabling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