City of London Police

DIGITAL SERVICES STRATEGIC ROADMAP 2020-23

Contents

Introduction

Residents, businesses, workers, and visitors expect the City of London to be well connected, both physically and digitally. Over 500,000 people (10% of the London workforce) are employed within the square mile -and they rightly expect to be able to access City services in a straight-forward, accessible manner. They want spaces that are technologically well-connected, vibrant, safe and sustainable.

The Police has an ambitious Policing Plan to significantly improve outcomes for the prevention and resolution of crimes. These ambitions will be realised in a world that is becoming more and more digital, with ordinary people and businesses having access to extraordinary computing power; using instant connectivity to access and add to vast stores of content and information; and wittingly or unwittingly sharing massive amounts of data about themselves, via their online activity and via widely-deployed sensors which whist improving live also make individuals and businesses more vulnerable to crime.

The year 2020, more than ever before, has elevated the importance of providing resilient services and working practices delivered through digital means, rather than paper based or location dependant processes. The events of 2020, specifically COVID-19, have shown that not all services have fully embraced the digital age. The Police continues to address these shortfalls, and through this strategy, will set out an approach to fully utilise the transformative role of technology in delivering modern, resilient and efficient Police services that meet our stakeholder's expectations and enabling and delivering technology to support the evolving role of a world class police service.

Digital Services Vision

Underpinning the Digital Services Strategic Roadmap for the Police is a common vision of people successfully working together in communities of interest to address matters of mutual concern and make change for the better.

Our proposed digital services vision sees the power of digital enterprise being used to create tangible human value by citizens, businesses and the officers of the City of London Police and other National Government and Public Sector bodies, who organize and act in communities of interest:

- to securely and reliably create, capture, communicate and act on information relevant to their community and the victims of crime.
- In all cases, digital denotes an approach to service that recognizes technologies as important means to human ends, via a combination of technology-enabled capabilities and collaboration-oriented cultures that promote continual review of performance, outcomes and experiences leading to learning and improvement.
- Putting digital into practice goes beyond traditional IT by focusing more on people and the value people get from embedding technology into their ways of thinking, communicating and acting to generate maximum value at least cost

This strategy document is underpinned by a key set of principles (Appendix A) and a Maturity Model (Appendix B). The Strategy alignment with the Policing Plan is shown in Appendix C. The Strategy is built on 4 pillars which is described below (see Appendix D).

1. Digital Policing

The Policing Vision 2025 sets out how digital policing will:

- Make it easier for the police and public to communicate with each other
- Improve digital investigations and intelligence
- Transfer all information with the Criminal Justice System (CJS) digitally.

Our Desired Outcomes:

The services and capabilities for Digital Policing is being developed by three key national programmes:

- Digital Public Contact (DPC) - will provide a simple, well known and reliable digital contact service between the public and the police that ensures the public are informed and digitally enabled.
- Digital Intelligence and Investigation (DII) - enabling policing to protect the public through preventing and detecting crime in a society that is becoming increasingly digital:
- Digital First (DF) - integrating digitised policing into the reformed Criminal Justice System, delivering the best service to the public
- Safe and secure online services consistent with National Cyber Security Centre (NCSC) standards

Key Priorities:

- Transform how we deliver digital services, working in multidisciplinary agile delivery teams capable of redesigning services from end to end, ensuring that a user's needs are considered and met throughout the whole process, and that back office systems and processes are integrated with front end delivery (see Appendix One);
- Review the technology underpinning our digital policing services, to ensure we have a resilient, supported and fit-for-purpose set of platforms that enable us to rapidly and sustainably build, maintain, and continuously improve digital services to better meet the needs of our users;
- Expand the use of the national policing self-service portal for all online services, positioning it as the primary gateway for all online services;
- Review and tighten up our criteria for permitting the creation of separate websites, with the aim of significantly decreasing the number of microsites and sub-domains;

Appendix E shows examples of Digital Policing in practice.

Appendix F shows how we will measure our success with our Digital Services Adoption

1. Technology (End User Computing)

End-user computing (EUC) is about bringing digital capabilities to life for an organisation, looking holistically at the breadth of the end-user experience and considering all the systems, tools and devices required to accomplish an individual's workload as flexibly as possible. The right technology can improve employee flexibility, productivity, innovation and customer satisfaction and management efficiency, and reduce errors and risk.

The IT Division supports approximately 1600 Police employees and members who use a mixture of Microsoft Windows 10 and Apple iOS end-user computing devices to fulfil their daily workloads. Most Windows 10 devices are laptops, although some fixed desktop computers are used for static desk requirements (e.g. reception areas). The IT Division is eager to put forth savings that contribute to the Police savings programme whilst delivering a leading end-user computing experience for the Police. Frontline Officers will benefit from new android devices and lightweight laptops. New radios will also be implemented that should be compatible with the new unified Emergency Network when this is launched in a few years.

Our Desired Outcomes:

For the end-user computing experience to be the best amongst its peers and rival those in leading private sector firms.

Act as an enabler for efficiency and value for money within IT and across all services.

Ensure secure and responsive digital and information solutions to the Police.

Drive forward a 'one team' focus to strengthen links between our teams and provision of a joined-up service.

The opportunity to open our doors to other Police Forces who can learn from our experience

Key Priorities:

Moving all our Official and Official Sensitive infrastructure into the Azure Cloud

Modernising and consolidating the tools and services used to manage end-user devices.

Standardising end-user computing devices across the technology estate to improve users experience and reduce support overhead.

Transitioning to continuous update and maintenance schedules (aka "evergreen") to improve user experience and consistently reduce risk.

Automating device provisioning and application deployment to reduce the time it takes to provision best-in-class devices.

Implementing a best-in-class, full-function self-service portal, for anytime access to services.

Introducing innovative devices and functionality that reduces the need to print and will reduce the time taken on signature-based paperwork.

Simplifying meeting room and collaboration technology to help make meetings more effective.

Migrating to a cloud hosted telephony solution. To improve flexibility and collaboration and to remove the legacy telephony hardware.

Reducing the need for physical network cabling, through greater adoption of WiFi infrastructure creating greater building independence and flexibility of working spaces particularly important in the aftermath of COVID-19.

2. Digital Workplace

The Digital Connected Workplace is the concept that organisations should use a more 'digital approach' to align technology, employees and business processes to improve operational efficiency and meet organisational goals. The underlying principle should be that our staff are able to operate effectively from anywhere, at any time.

Following the COVID-19 pandemic the importance of resilient, stable and easy to use technology for staff from any location has never been more important. The organisation realised a shift to more digital ways of working literally overnight, therefore our ambitions around digital and cultural change should not be limited.

For the Police, significant progress has been made through the IT Modernisation Programme (2019-2020) which sees 80% of staff move to using laptops and tablets as their main devices, allowing for more agile and flexible working. The Programme also moved the organisation to Office 365, an evergreen approach to Microsoft's traditional productivity tools, which also now includes functionality around document management, audio and video conferencing, collaboration tools, online forms and business intelligence.

Our Desired Outcomes:

- All staff have fit for purpose Police technology and line of business applications, which support efficient, resilient and streamlined business processes;
- All staff make effective use of cloud collaboration and productivity software to communicate, safely share and store information, and work with increasing efficiency;
- All staff can work effectively from anywhere at any time, including fast and reliable wired and wireless network and telephony access in all corporate office locations;
- All staff are confident in their use of technology and have access to the right information to measure service performance and make well-informed decisions;
- Senior Officers and Members exemplify and champion digital expertise and culture;

Key Priorities:

1. Continue to drive adoption of digital workplace tools, identifying opportunities for efficiencies, reductions in duplication and manual handling, as well as challenging poor practice or outdated ways of working;
2. Promote SMART working to develop a more flexible and resilient workforce, utilising existing tools to increase productivity, encourage an improved work-life balance and efficient utilisation of Police properties through hot desking and the provision of more collaborative office space;
3. Seek out opportunities to use new and emerging technologies such as robotic process automation and machine learning to automate low value tasks and improve operational efficiency.

3. Technology (End User Computing)

End-user computing (EUC) is about bringing digital capabilities to life for an organisation, looking holistically at the breadth of the end-user experience and considering all the systems, tools and devices required to accomplish an individual's workload as flexibly as possible. The right technology can improve employee flexibility, productivity, innovation and customer satisfaction and management efficiency, and reduce errors and risk.

The IT Division supports approximately 1600 Police employees and members who use a mixture of Microsoft Windows 10 and Apple iOS end-user computing devices to fulfil their daily workloads. Most Windows 10 devices are laptops, although some fixed desktop computers are used for static desk requirements (e.g. reception areas). The IT Division is eager to put forth savings that contribute to the Police savings programme whilst delivering a leading end-user computing experience for the Police. Frontline Officers will benefit from new android devices and lightweight laptops. New radios will also be implemented that should be compatible with the new unified Emergency Network when this is launched in a few years.

Our Desired Outcomes:

- For the end-user computing experience to be the best amongst its peers and rival those in leading private sector firms.
- Act as an enabler for efficiency and value for money within IT and across all services.
- Ensure secure and responsive digital and information solutions to the Police.
- Drive forward a 'one team' focus to strengthen links between our teams and provision of a joined-up service.
- The opportunity to open our doors to other Police Forces who can learn from our experience

Key Priorities:

4. Moving all our Official and Official Sensitive infrastructure into the Azure Cloud
5. Modernising and consolidating the tools and services used to manage end-user devices.
6. Standardising end-user computing devices across the technology estate to improve users experience and reduce support overhead.
7. Transitioning to continuous update and maintenance schedules (aka "evergreen") to improve user experience and consistently reduce risk.
8. Automating device provisioning and application deployment to reduce the time it takes to provision best-in-class devices.
9. Implementing a best-in-class, full-function self-service portal, for anytime access to services.
10. Introducing innovative devices and functionality that reduces the need to print and will reduce the time taken on signature-based paperwork.
11. Simplifying meeting room and collaboration technology to help make meetings more effective.
12. Migrating to a cloud hosted telephony solution. To improve flexibility and collaboration and to remove the legacy telephony hardware.
13. Reducing the need for physical network cabling, through greater adoption of WiFi infrastructure creating greater building independence and flexibility of working spaces particularly important in the aftermath of COVID-19.

4. Police Modernisation and Digital Services Delivery

Policing does not operate in a vacuum and cannot stand still in the increasingly digital world we work and live in. The challenges and opportunities that digital disruption present to policing are rapidly becoming defining issues for the service.

To protect people from harm in our rapidly changing world the Police service must modernise. We will enable capabilities to address the digital challenge and deal with the complexity of modern criminality through the exploitation of new technologies and data. Modernisation of the Police service will require a significant change in the City policing system.

Outcomes	Priorities
Multi Chanel Access - for citizen interactions, information, data and interactions across departments and forces whilst maintaining trust of citizens through ethical use of data	• Enhance physical experiences through digital means wherever possible easy and frictionless. • Harness shared data and connected devices ethically and securely. • Use digital technologies to enable the public to protect their communities.
Data for proactive Policing - We will harness the power of digital technologies and behaviours to identify the risk of harm and protect the vulnerable in the physical and digital world. We will deliver earlier, more precise and targeted information to enable proactive policing approaches and early interventions	• Translate evolving definitions of threat, harm and risk (THR) into digital formats that complement human judgement. • Use digital tools to rapidly identify harm related behaviours in order to target interventions • Use digital tools to disrupt criminal activity. • Design and deliver digitally enabled interventions that work across boundaries.
Digital Skills and Capabilities – Investment in people, from leadership through to the front-line, to ensure they are equipped with the right capabilities (knowledge, skills and tools) to deal with increasingly complex crimes. Establish digital leadership and ways of working to allow our workforce to focus on critical and value-adding activities.	• Provide officers and staff with the digital tools they need. • Establish new digitally enabled, dynamic workforce models. • Maximise the benefits of the investment in Police IT Modernisation changing ways of working to maximise crime detection and efficiency • Develop a digitally literate workforce and leadership
Digital Relationship with the Private Sector – Enable the strengthening of relationships with the private sector to empower those organisations to appropriately share in public safety responsibilities.	• Define expectations through open dialogue with the private sector but also with input from citizens. • Build awareness of digital threat, harm and risk. • Build awareness of digital threat, harm and risk. • Support the private sector role in digitally enabled public safety sharing CCTV and information to detect and prevent crime
Digital Relationship with the Public Sector and Criminal Agencies - We will enable a philosophy of openness and deepen our collaboration with our public sector partners and criminal justice partners to jointly design and tackle complex public safety issues. This means sharing data insights and making use of digital tools to work more effectively across the public safety system, ensuring we do so in an ethical way to safeguard public trust.	• Deepen our collaboration with public sector agencies to unlock effectiveness. • Develop 'fluid' information and insight exchange between public sector agencies, within appropriate ethical and legal boundaries. • Support the creation of integrated digital public services for public safety
Action Fraud and the National Fraud Intelligence Bureau (NFIB) - As the designated UK's lead force for economic crime the force needs to improve access, reporting ad monitoring by citizens of reported Cyber Fraud. The Force needs to replace the back-office system in the next 2 years for managing Action Fraud and more immediately improve the data analytics and heuristic models for filtering the cases that are managed through NFIB	• Deepen our collaboration regional forces and private sector with integrated information sharing • Develop faster better self-service reporting and monitoring • Procure a new back office system with better integrated data analytics for crime resolution and prevention

5. Safe and Secure City

The Initial Smart City Strategy set out a model for delivering a competitive future City of London using smart-enablement and innovation. This model was structured using the corporate vision and the three key themes of People, Place and Prosperity, with smart-enablement and innovation as the foundation for this structure, cutting across all future city activities as an enabler of change. The overarching aim of the 'Smarter City' work is to ensure the City's continued competitiveness as a thriving international financial and business centre.

The Smarter City approach has now evolved into the Secure City Programme.

Our Desired Outcomes:

- The Secure City Programme (SCP) is a joint programme between the City Corporation and the City of London Police that seeks to enhance the security of the Square Mile and provide benefits in terms of transport planning & monitoring.

Our Priorities

- the replacement of legacy & life-expired on-street analogue CCTV cameras with high definition 4K digital cameras.
- the installation of new CCTV cameras to cover priority 'blind spot' locations, including parts of the City's Thames Bridges, ensuring such additional coverage is proportionate and appropriate
- the implementation of appropriate back office IT systems to accept and manage these new digital CCTV inputs, including video analytics to support both Police and the City of London Corporation requirements and a system for secure data storage
- the integration of existing stand-alone CCTV networks from other police forces and City of London Corporation locations into this system.
- the creation of additional CCTV camera coverage on the City's bridges and Thames riverside focused on vulnerable people
- integration of back office IT system with a series of wider policing requirements to create a holistic Security Management System, incorporating incident management, resource deployment and computer aided dispatch
- the establishment of a new permanent home for the Joint Command & Control Room which will be the physical staffing space to host the monitoring and management of these systems
- the ingest of further CCTV systems from third party premises around the Square Mile

6. Data and Information Management

Information management is the formalised collection, storage, analysis, use, sharing and disposal of all types of information, from data through to knowledge.

This can mean gathering, creating, filtering and disseminating information, using it to support decisions and actions, or conserving or disposing of it. Recent research across the Corporation shows that the way in which information is managed varies significantly. Poor information management incurs significant costs in terms of ill-informed decision-making, missed opportunities and missed threats. Even where the right information is used properly, there is often effort and delay in obtaining and verifying it.

The more we know and understand, the better we can decide and act, particularly for our stakeholders. Improper gathering, disseminating and analysing of information can put those people at risk. That's why data protection legislation has been passed to regulate this, with stiff penalties for contraventions.

Good information management provides benefits across the Corporation and for our stakeholders. Its principles are relatively straightforward, but its implementation is made complex by the breadth and depth of its applicability and interdependencies. This is why a strategic approach is required.

Our Desired Outcomes:

- The Police has the necessary awareness, tools, skills and culture to promote a set of behaviours and values which understands and manages good information management practice.
- The Information estate is safe, relevant, accurate, reliable, used and trusted.
- The Police derives real value and benefits from the use of information, data, analysis and modelling.
- The Police has sufficient checks, balances and oversight to ensure the successful implementation of this strategy.

Key Priorities:

14. We will educate, encourage and enable staff to store a single version of information that can be added to and amended. We will discourage duplication and encourage information reuse and repurposing. We will insist on safe disposal of information when no longer needed.
15. We will provide the information required – securely, quickly, easily, accurately, conveniently, consistently, and transparently. Systems will be procured, designed and developed to enable effective information sharing, analysis and presentation.
16. We will develop and nurture new information management values and behaviours, including a drive to continually improve based on experience and research. We will encourage an approach of curiosity and challenge in the use of our information. Departments will be given the skills and capability to lead and champion this ambition.
17. Information and intelligence will be securely stored and protected and only exchanged according to national polices guidelines and standards.

7. Capabilities for the New Digital Norm for the Police

Capabilities are the 'things that the Organisation needs to do' in order to deliver our services to our stakeholders.

Capabilities are delivered irrespective of organisational structure differences across the organisation, and therefore serve as a useful tool to highlight the impact of digital on forces.

There are obvious need to train staff on digital tools such as the new collaboration tools we have provided and will enhance in coming months and years. There is also a need to improve the data literacy and capability of staff.

Many of the capabilities that we will need to focus on are detailed in the table below:

Capabilities	Skills
Knowledge provision and disruption	The provision of timely, contextual and accurate crime prevention advice based on insights from analytics; as well as the use of digital disruption techniques to unsettle identified criminal activity.
Reporting	The ability to receive and create incident and intelligence reports through multiple channels from the public, our partners and the front-line.
Data management and sharing	The storage of data in accredited data management systems which comply with national data management and handling standards and processes – allowing interoperability between forces and partners.
Data acquisition	The ability to acquire data, maximising the potential provided by digital technologies in support of public safeguarding and crime prevention.
Data preparation	The ability to access, cleanse and manipulate vast amounts of data efficiently and effectively and make this available for decision making processes, analytics and intelligence development activities.
Process automation	The ability to automate predictable processes, as well as automated demand analysis and response to improve quality of decision-making, tasking and assessment.
Analytics	The ability to provide insights from acquired data in the form of predictions, estimations and conclusions.
Infrastructure and technical governance	Infrastructure which provides scalable storage and computing capabilities whilst enabling interoperability between forces and partners.
Continuous improvement and innovation	The ability to continuously improve and innovate, promoting a culture of change / adaptation at the pace of the operational environment.
Service sustainment	An effective governance structure in place which leads the delivery of projects. Assuring compliance with standards and policy for in-flight and newly implemented projects. Undertaking benefits management to ensure projects are delivered to the required scope, time, quality and budget.

8. Action Fraud

In his recent report, by ex-Met Police Deputy Commissioner Sir Craig Mackey, found fraud now accounts for one-in-three crimes - but just 2% are detected and despite nearly 2,000 fraud offences being committed daily in England and Wales, just one in 50 is prosecuted.

In his report Sire Craig Mackay found that for the investigation of fraud to be effective at a national level, three distinct activities need to work well together. The 'first contact' services of Action Fraud set the tone for the victim experience and gather together lines of enquiry for investigators. The NFIB analyses and develop cases before referring them to forces for investigation. In turn, the capacity and expertise need to be available in police forces to investigate thoroughly and serve victims professionally. It is only when these interdependent stages of the process join up effectively that victims will have confidence in the system and fraudsters will be brought to justice.

With the volume of Fraud increasing and an inadequate IT system to investigate and triage the cases for further investigation by the National Fraud Intelligence Bureau (NFIB) a new Action Fraud and National Fraud Intelligence system needs to be procured and implemented in the next 2 years.

Outcomes

Action Fraud and NFIB - As the designated as the UK's lead force for economic crime the force needs to improve access, reporting ad monitoring by citizens of reported Cyber Fraud. The Force needs to replace the back-office system in the next 2 years for managing Action Fraud and more immediately improve the data analytics and heuristic models for filtering the cases that are managed through NFIB and distributed to local forces to investigate.

Priorities

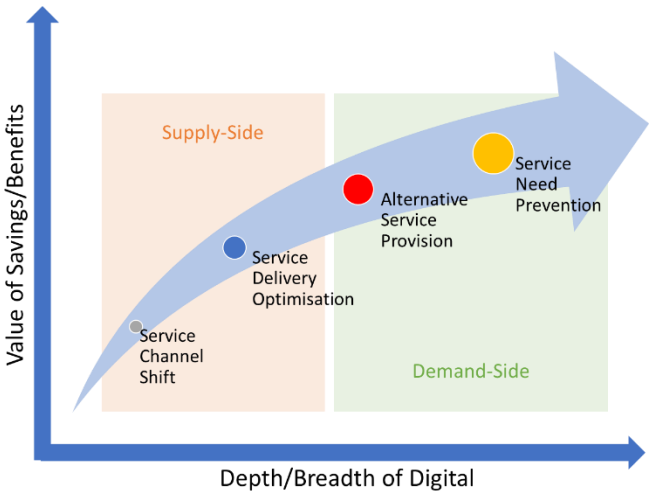
- Deepen our collaboration regional forces and private sector with integrated information sharing
- Develop faster better self-service reporting and monitoring
- Provide an interim transition arrangement for the existing to the new system
- Procure a new back office system with better integrated data analytics for crime resolution and Prevention.
- Develop a Victim centric fraud platform

See Appendix G for Strategic Roadmap

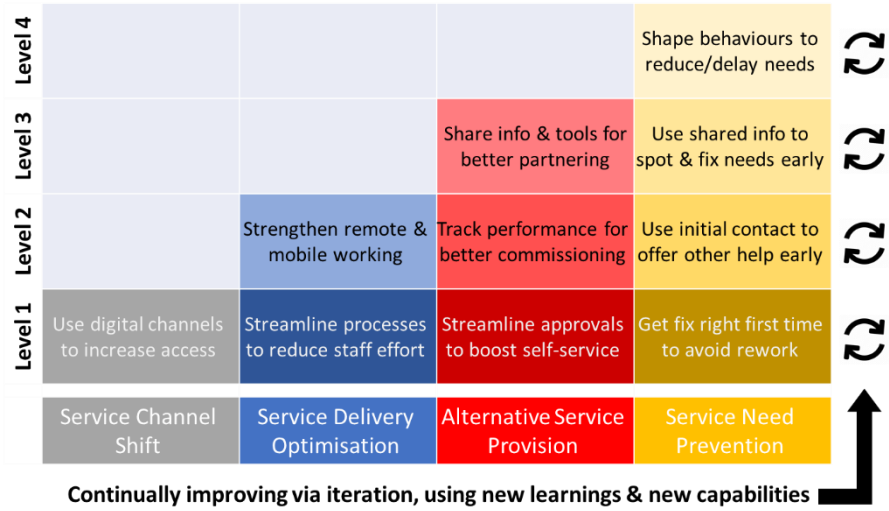
APPENDICES

Appendix A – Digital Services Maturity – What Does Good Look Like?

The Corporation can best use its resources and authority to address needs and meet challenges by working collaboratively, both internally and externally. The benefits of this are suggested in the value curve diagram at right.



This means being as efficient as possible in supply-side fulfilment, where the Corporation can use its resources across different services to minimize effort while maximizing impact; and being as effective as possible in demand-side management, where they can use their authority in partnership with others to prevent, or at least minimize, need.
This curve, which is purely indicative and not based on specific data, reflects the concepts that prevention is better than cure, and that a problem shared is a problem, well, if not halved, then at least reduced.



The diagram at left depicts a maturity model based on the value curve above. The maturity level increases with degree of digital adoption, as evidenced by new initiatives and changing behaviours that lead to greater value/saving.

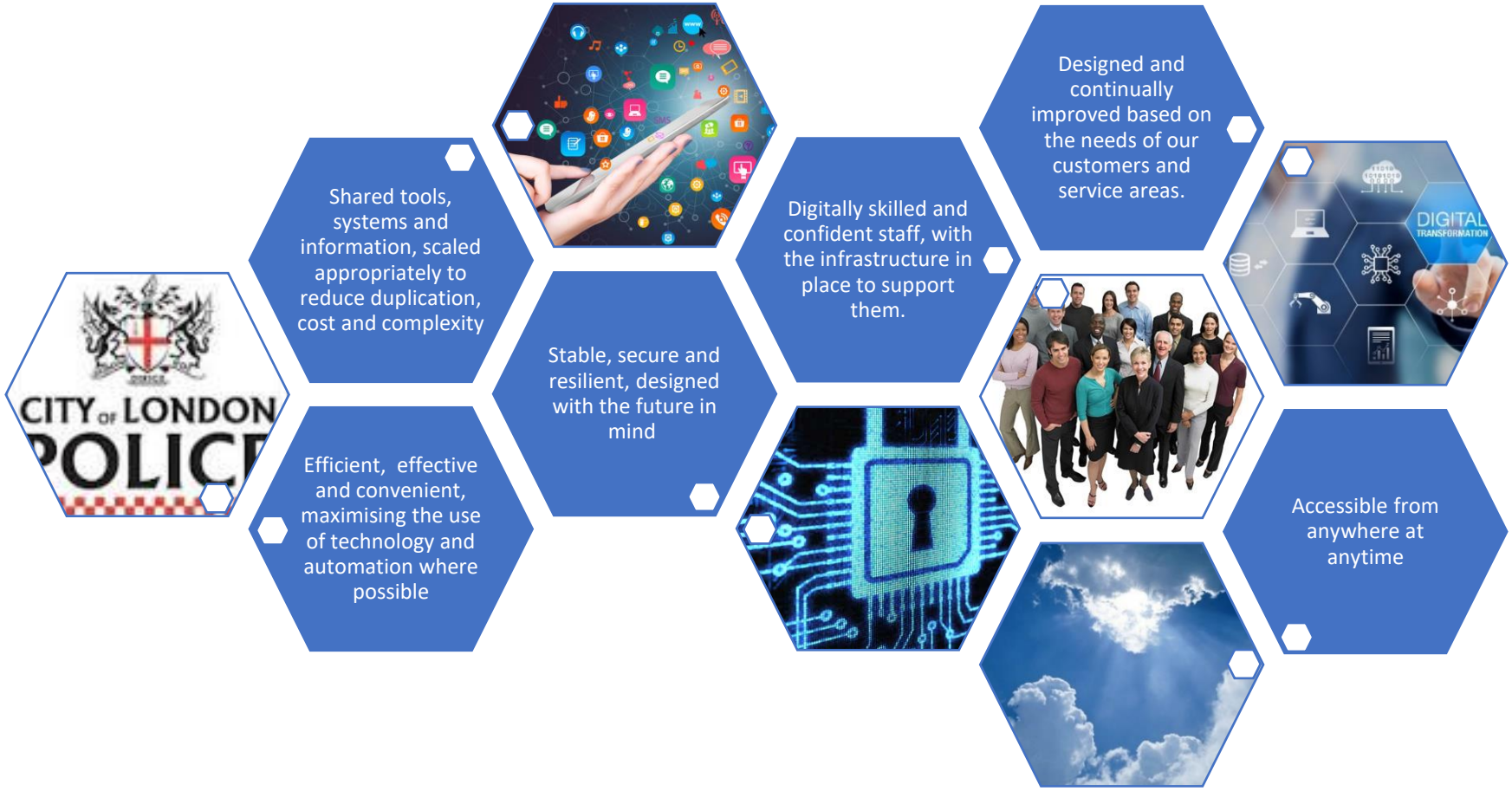
Different services and communities may progress through the maturity levels at different rates in the different stacks (Service Channel Shift, Service Delivery Optimisation, Alternative Service Provision and Service Need Prevention). The model reflects a continual improvement approach, moving upwards a step at a time in different areas, and learning as we go.

Measuring Digital Maturity

Progress in delivering the strategy will be tracked through various measures that reflect underlying changes in values and behaviours and improvements in technology, processes and skills. Targets will be set for each measure, with its current value, direction of travel and the key factors influencing the velocity of change being presented to stakeholders via an online dashboard. The initial measures, targets and velocity factors are shown in Appendix F.

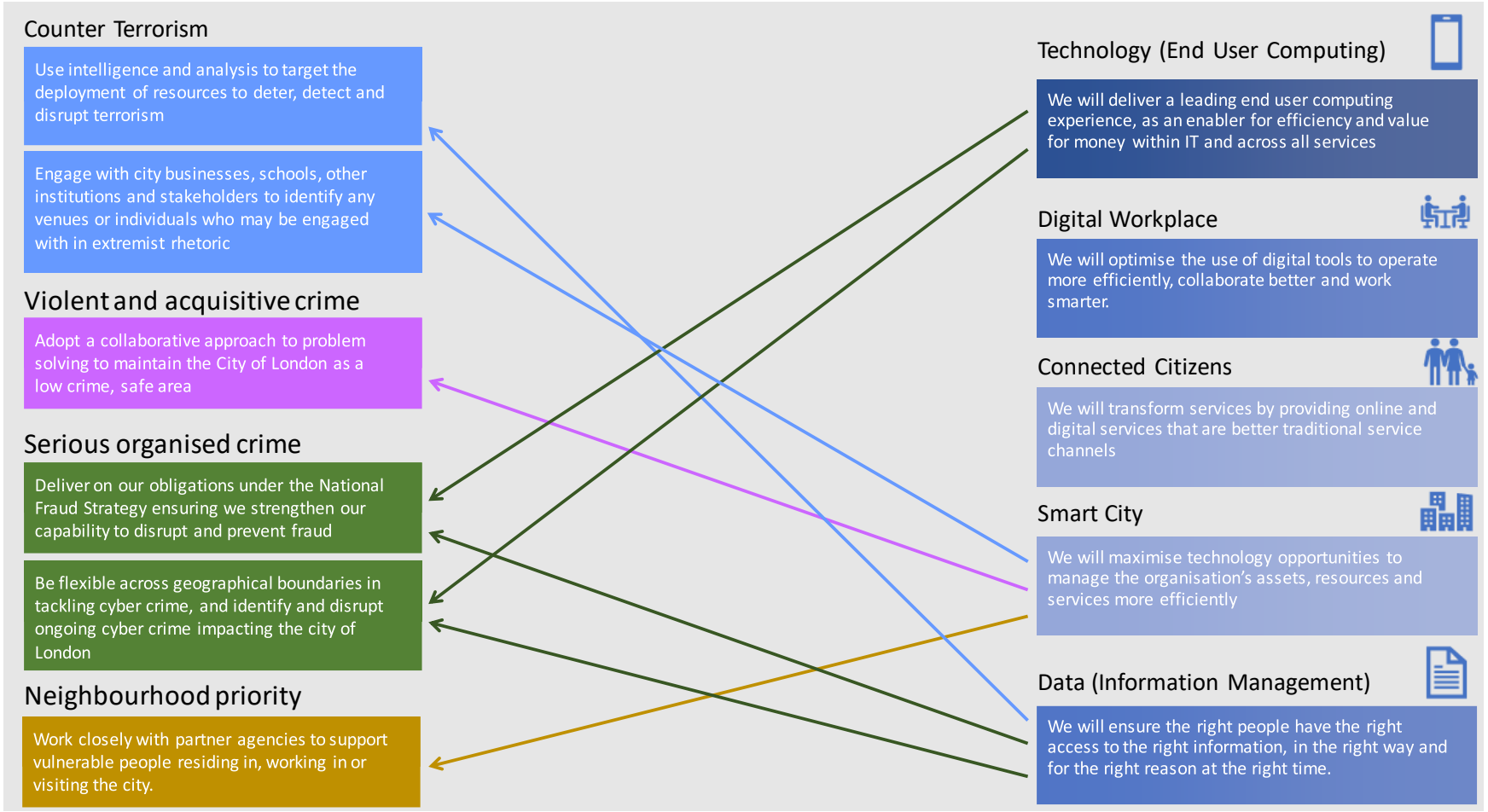
Appendix B – Digital Services Principles

The strategy aims to deliver leading Digital Services for the Corporation. For the purposes of this strategy, Digital Services are defined by the following principles:



Appendix C – Strategy Alignment with the Policing Plan

In delivering this strategy we will ensure benefits derived from activity is linked from our five key pillars back to the Police Plan for 2020– 23. The below shows at a high level how each pillar will directly contribute to the Police vision; dedicated to a vibrant and thriving City, supporting a diverse and sustainable London within a globally successful UK.



Appendix D – Digital Working in Practice – Examples for the Police

Supporting CoL and CoLP Officers

Becoming digital will require CoLP officers to acquire, practice and improve digital skills, becoming comfortable with digital tools and culture. The Digital Strategy will seek to support this personal growth through instituting just-in-time, online, on-the-job training, backed up by scheduled, formal, classroom training where needed. It will also look to upskill selected individuals to act as digital coaches and mentors embedded in the services and business units, while enabling and encouraging collaborative and ad hoc learning and support across the workforce.

CoLP Supporting Officers – Public Service Entrepreneurship

The concept of *public service entrepreneurship* suggests that some of the more successful elements of commercial entrepreneurship can be applied in public service settings. This builds on aspects of digital culture, including service co-design and output co-production, and is made more efficient and effective through using digital capabilities.

Key elements include seeking out unmet needs, understanding why they exist and planning how to meet them; responding to public service consumerism; incrementally and iteratively improving existing services; experimenting to gain real-world learnings; taking appropriate risks; and making best use of resources.

A digital approach can help in all these areas by supporting communication, co-ordination, mobile working and access to up-to-date information, which together enable a lean and agile approach to service design and improvement.

CoLP Frontline Police Officers – Evidence and Intelligence

CoLP frontline officers need to gather evidence quickly, accurately and comprehensively; securing the evidence while sharing it as needed; connecting the dots to create reliable intelligence; and communicating that intelligence to those who can make best use of it are all critical to good policing.

Specialist mobile hardware, e.g. fingerprint scanners, and software, e.g. digital discovery software, can greatly speed up evidence gathering and processing, with secure digital evidence repositories and case files making it easy to keep track of and share growing bodies of evidence and case notes for joined-up policing and prosecution.

Secure, flexible and mobile access to and integration with national police intelligence systems gives officers at all levels the means to jointly identify, track and follow-up on threats, leads and suspects. Meanwhile, data analysis across crimes, demographics and cross-government policy changes can help to predict and prevent new risks and issues.

Appendix E – Measuring Digital Adoption

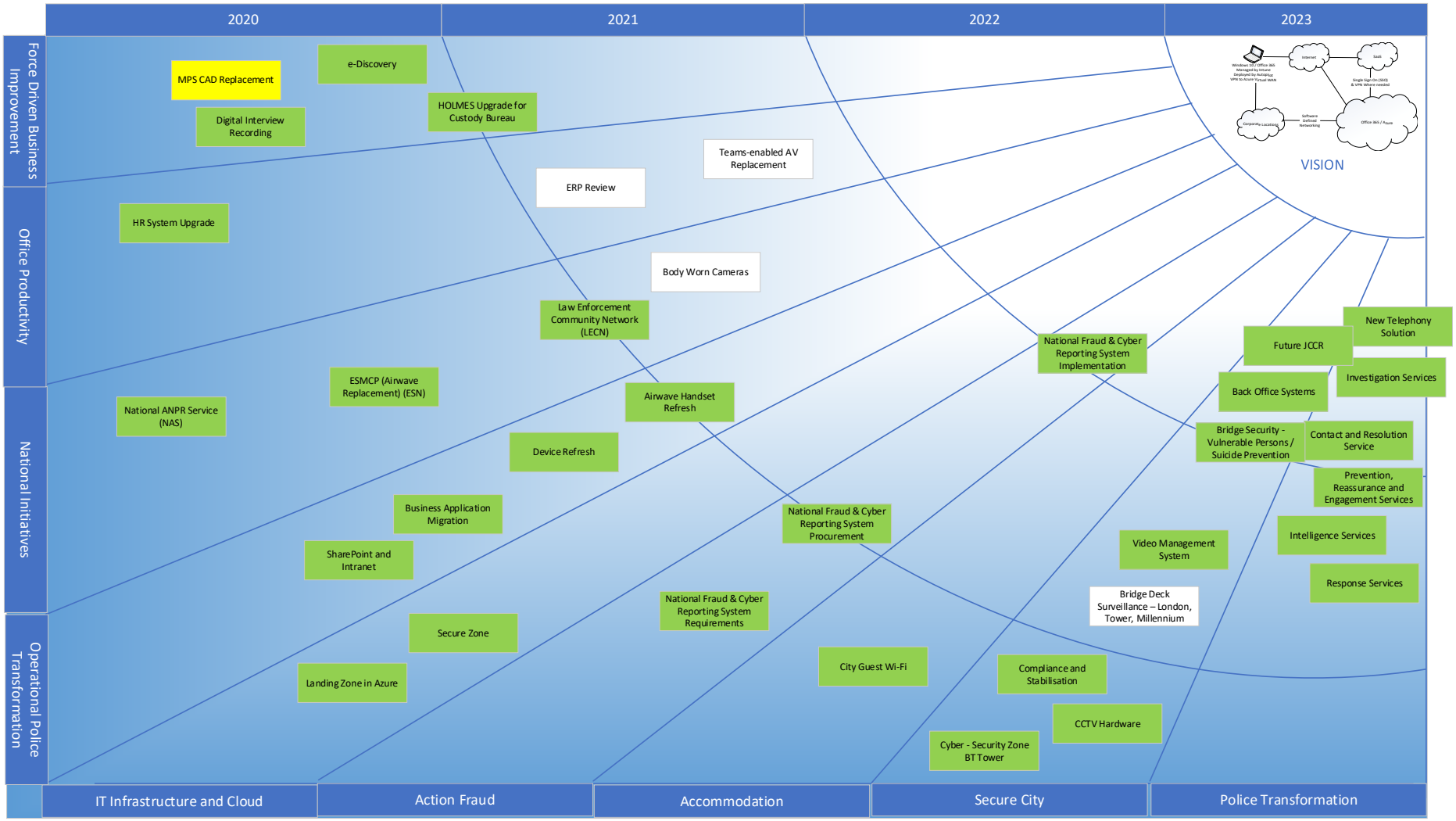
The baseline figures for relevant measures will be established early in the strategy implementation process.

Targets in red, these are best practice numbers, that may need to be staggered targets during the four-year period to show positive incremental change. These are being worked up in line with our business plan for consistency.

	Measurement	**Description**	**Outcome Impact**	**Target**
1	Digital Adoption in the Organisation measured by Channel Shift, **Reduction in Printing** and Staff use of SharePoint	Printing reflects comfort with onscreen reading and online sharing of documents *See second table for channel shift and changes in use of SharePoint*	Reduced costs of printing, and paper storage and disposal for the organisation, less time spent by staff in printing, filing and retrieving documents, less staff tie to office print facilities	Decreases to 25% of baseline
2	Cloud Migration achieved	This reflects all storage and compute needs being met via the Azure infrastructure	Reduced infrastructure costs for the organisation, increased reliability of storage and compute provision	90%-100% depending on ability of business systems to use Azure
3	Percentage of *(traditionally office-based)* workforce working 3 or more days a week from home	This reflects effectiveness and efficiency of online sharing and meeting	Better work-life balance for staff, reduced office space and facilities costs for the organisation	Increase to 50% of all qualifying staff
4	Performance against annual savings target set	This reflects improved cost and demand prediction, monitoring and management	Reduced costs for the organisation	Targets 100% met
5	Weighted average of elapsed time to fulfil IT service request	This reflects degree of cloud migration, IT standardisation and process automation	The organisation can more nimbly deal with changes to demand, staffing and cost pressures	Decrease to 75% of baseline
6	Percentage of victim reports made online	This reflects the percentage of public services available online and their convenience compared to other channels	Members of the public are conveniently registering their services needs while the organisation enjoys reduced costs in registering them	Increase to 90% of all requests

7	Percentage of staff service requests made online	This reflects the percentage of staff services available online and their convenience compared to other channels	Members of staff are conveniently registering their services needs while the organisation enjoys reduced costs in registering them	Increase to 90% of all requests
8	Volume of file attachments sent internally via email	This reflects the convenience of other file sharing channels, e.g. SharePoint	Files version control is better managed, email and file storage needs are reduced, managing feedback is eased	Decrease to 10% of baseline
9	Volume of email sent internally	This reflects the convenience of other channels, e.g. Teams, and need to keep message records	Reduced cost of email storage, easier for staff to manage their email	Decrease to 50% of baseline
10	Percentage of staff working away from office 3+ days a week	This reflects effectiveness and efficiency of online sharing and meeting and of mobile working	Better work-life balance for staff, reduced office space and facilities costs for the organisation, more relevant staff in the community	Increase to 75% of all staff
11	Percentage of public service requests fulfilled without direct service team intervention	This reflects degree of information reuse and of process simplification and automation achieved and of validation and approval still needed	Increased convenience and speed for requester, reduced processing costs for organisation	Increase to 50% of all requests
12	Percentage of staff service requests fulfilled without direct service team intervention	This reflects degree of information reuse and of process simplification and automation achieved and of validation and approval still needed	Increased convenience and speed for requester, reduced processing costs for organisation	Increase to 75% of all requests

Appendix F – CoLP Strategic Roadmap



Appendix G - Glossary of Terms Used in Roadmap Sunray Diagrams

ADFS	Active Directory Federated Services – part of the IT infrastructure that manages and shares relevant user and device identity and configuration information across organisations that have chosen to work together this closely
AI	Artificial Intelligence – the ability for software to react to information and make decisions in a way that may appear similar to some forms of human intelligence; typically based on human-programmed algorithms and machine-learned rules of thumb (see glossary entry for *ML*)
ANPR	Automatic Number Plate Recognition – an automated system that identifies a vehicle and its owner by reading the vehicle's registration number from a digital image of its number plate and then searching for that number in the Driver and Vehicle Licensing Agency database
API	Application Programming Interface – simplified software methods for accessing the functionality of complex software, used to query and command that software by other software; one of the key ways that software systems can be integrated with one another and enhanced by third-party software developers
AV	Audio-Visual – facilities (cameras, projectors, screens, microphones, speakers, headphones, etc.) and associated methods for using sight and sound to support human communications such as presentations, meetings and training
Azure	Microsoft's brand name for its suite of cloud computing services (see glossary entry for *Cloud*), used in the roadmaps to refer to the subset of these services that provide infrastructure as a service (network, compute and storage)
BYOD	Bring Your Own Device – an approach to providing a user with network, compute and storage services for work by making use of equipment and services that the user already has access to (and often owns and funds) for non-work purposes, e.g. personal mobile phone, home computer
Cloud	Refers to computing resources provided as large-scale shared services, often off-premises and by an external supplier, where the end-users treat the services almost as utilities, paying only for what they use and not having to manage their production and delivery; typically offers economies of scale due to fixed costs of services being shared with other parties, and greater robustness due to the large amount of shared resources allowing for more redundancy
CMDB	Configuration Management Database – a database and methods for managing devices, software, networks and users by managing the information that defines them; changes in the real-world affect CMDB contents and changes to CMDB contents affect the real world
CRM	Customer Relationship Management – a system and methods for an organisation to manage its relationships with its customers (or 'citizens' in

	public sector contexts); typically centred on a database tracking customers' details and their interactions with the organisation
E5	A tier of Microsoft enterprise licensing for its software, a higher tier than E3 at which CoL and CoLP are currently licensed; a higher tier costs more per user but includes access to more software, has fewer usage restrictions and/or offers deeper discounts from list prices
ERP	Enterprise Resource Planning – a suite of software that allows better overview and joined-up management of organisational resources (funds, people, assets, consumables) as they get involved in processes such as payment, join/move/leave, maintenance and production
ESMCP	Emergency Services Mobile Communications Programme – the Home Office-led programme of work to deliver the Emergency Services Network (see glossary entry for *ESN*)
ESN	Emergency Services Network – the Home Office-sponsored high-performance voice and data network and associated services that support mobile working by the police and other emergency services
HOLMES	Home Office Large Major Enquiry System – the central system, accessible by all police forces, for recording, sharing, connecting and analysing information relating to complex criminal investigations, which is undergoing significant improvement and expansion
ML	Machine Learning – the discovery of scenario-specific patterns by a computer system using sufficient processing power to analyses large quantities of scenario data, and resulting in pattern-matching rules of thumb that computers can use to make decisions and predict outcomes
Intune	Microsoft's brand name for its system for managing configuration, security and use of end-user devices such as laptops, tablets and mobile phones; includes delivery of software packages and operating system updates
iOS	Apple's brand name for its mobile operating system used on its iPhone and iPad devices, which make up much of the Corporation's mobile fleet
ITSM	Information Technology Service Management – principles, methods and systems for designing, implementing, operating, controlling and retiring one or more IT services, informed by service user and service owner needs in the context of business and technology strategy
SaaS	Software as a Service – a model of software provision where, rather than buy software outright and run/manage it on their own infrastructure, the customer pays the supplier per unit consumption to remotely access and use the software as it is run/managed on supplier infrastructure
SCCM	System Centre Configuration Manager, Microsoft's system for managing configuration, security and use of data centre and end-user devices; includes

	delivery of software packages and operating system updates; Intune is taking over for end-user devices (see glossary entry for *Intune*)
SIEM	Security Information and Event Management – principles, methods and systems for automatically and continuously collecting and analysing security-relevant data logged about network, device and user activity to help identify security threats and investigate security incidents
SOA	Service Oriented Architecture – an approach to system design that exposes system functionality as different small specific services that follow common standards and can be accessed independently of one another; this makes it easier to link different bits of functionality from different systems together to create tailored solutions, and to replace functionality from one system with better functionality from another system by swapping one standardised service for another
UC	Unified Communication – a single system for a user to access, create, transfer and manage all their inbound and outbound communications across various media and channels (e.g. email, chat, voice, video and internal, external, work, personal) more conveniently and productively
WAN	Wide Area Network – a data network that connects computer systems at many sites spread across a large geographical area; in contrast, a Local Area Network connects computer systems located at a single site, e.g. a building or floor