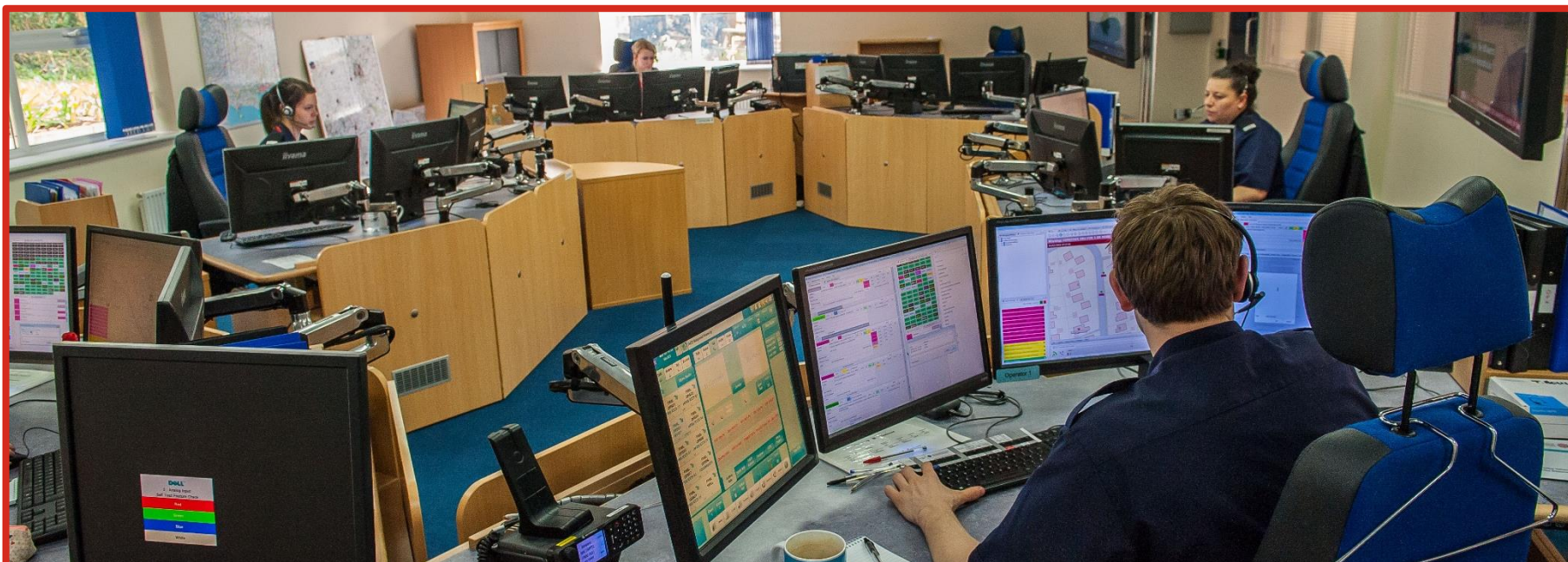




DORSET & WILTSHIRE
FIRE AND RESCUE



ICT Strategy

2021-24

PASSIONATE ABOUT
CHANGING & SAVING LIVES

ABOUT THIS STRATEGY

To help make Dorset and Wiltshire a safer place to live, work or visit, we need to ensure that all our efforts and resources are focused on having the right people, in the right place, at the right time, with the right skills and equipment to prevent and to respond to emergencies when they happen.

To help guide our thinking, and to keep ahead of an everchanging world, we regularly review both our external operating environment, as well as carrying out an internal analysis of where our Service needs to be.

Our Strategic Assessment of Risk (SAR) supports the development and review of our Community Safety Plan (CSP) and organisational strategies. This is then translated into on the ground action at department, station and team level through our Service Delivery Plan (SDP), which is underpinned by a comprehensive performance framework.

This strategy therefore sets out how our Service will improve over the next three to five years to further strengthen our Information, Communication and Technology (ICT).

This strategy also underpins the Government ICT Strategy and supports both the Networked Fire Control Services Programme (NFCSP) and the Emergency Services Mobile Communication Programme (ESMCP) and subsequent Emergency Services Network project (ESN).

PURPOSE

The purpose of this strategy is to set out a long-term pathway to deliver against the ambition set out the Community Safety Plan and the policies agreed by the Authority.

In developing this document, we have considered:

- The problems and critical issues we need to respond to.
- The policy objectives set out by the Authority.
- The priorities and our capacity to achieve them.

This plan is structured to provide a picture of where we are now, and the context for the journey we intend to go on. It outlines what we want to achieve and provides a picture of our intentions over the next three to five years.

This strategy will be dynamic and will be managed by the Director of Service Support and monitored through the Strategic Leadership Team and Members through our performance management arrangements.

STRATEGIC FOCUS

- Information Governance & Security.
- Operational Communications & ESN.
- ICT Resilience.
- Technology Management.
- Digital Transformation.
- Business Intelligence and Data Management.

HMICFRS

This strategy aligns to and informs the following Key Lines of Enquiry:

- KLOE 6: How well do we use resources to manage risk?
- KLOE 6.11: To what extent do we demonstrate effective management of information communication and technology?
- KLOE 7: How well are we securing an affordable way of managing the risk of fire and other risks now and in the future?
- KLOE 7.4: How are we planning to invest in future innovation and use technology and new ways of working?
- KLOE 13: Are effective governance and decision-making arrangements in place?
- KLOE 13.3: How effective and efficient are we at managing data?

Strategic position

Strengths:

- Continued development of modern and reliable ICT infrastructure and technology to support availability of on-call appliances for efficient and effective operational response (SAR).
- Continued work with the Networked Fire Control Services Partnership (NFCSP) (SAR).
- Flexibility in being able to quickly adapt, react and develop to the changing business needs.
- Business led ICT investments and arrangements.
- Information security processes and controls in place.
- Effective information governance and assurance arrangements.
- Well defined roles, responsibilities and governance for Information Asset ownership.
- User focused technology and digital access to all staff.
- Technology to support operational capability on station and in appliances.
- Corporate management of key information systems for decision making, consistency and managing performance.
- Digital Transformation programme delivering and supporting the adoption of Office 365.

Weaknesses:

- Financial uncertainty for the Service and its partners (SAR).
- The Service needs to engage and resource the emergency services mobile communications programme to improve future resilience of communications and incident management (SAR).
- The recruitment and retention of skilled ICT staff will remain increasingly difficult.
- Continued changes in technology and expectations within limited resource base.
- A need to migrate off legacy systems onto a more generic and future proofed Office 365 and SharePoint platforms to improve value for money, efficiency, resilience, and security.
- A need to reduce passwords and user names across management systems.
- Meeting the continued challenges of cyber security standards and codes of connection.
- A need to improve data and system integration and visibility and understanding for end users to interpret and inform decisions.

Opportunities:

- The outcomes and findings of the Grenfell Tower inquiry is likely to have a significant impact upon the fire sector particularly creating opportunities to make best use of technology to support new ways of working (SAR).
- Make maximum use and achieve value for money of what we have in resources, considering and continually reducing its environmental impact (SAR).
- Environmental scanning for multi-use products, to achieve better value for money.
- Better understand and improve the capability of our workforce and our one team approach (SAR).

Threats:

- Increasing threat of cyber-attacks.
- Maintaining a skilled resource team against a fast-moving technological landscape.




- Maximising the benefits of SharePoint & Office 365 to improve ICT skills, collaborative document development and management reducing in duplication and increase in 'only enter it once'.
- Emergency Services Network and associated national project roll out.
- Championing the use of data to drive decision making through better use of knowledge and information.

Strategic challenges

- Long term vision and future planning for use of technology to improve operational functionality and effectiveness.
- Maintaining pace with technological change within limited resource base.
- Further maximising the value for money opportunities arising from the ICT estate and national projects.
- Maintaining an ICT infrastructure that protects the confidentiality, integrity and availability of our information.
- A need to improve data and system integration and visibility and understanding for end users to interpret and inform decisions.

Information Governance and Security

With a focus on  Equality, Diversity & Inclusion and  Environmental Sustainability

Where we are now	Where we will be in three years	What we will do
<ul style="list-style-type: none"> • Cyber action plan being delivered to achieve compliance with National Cyber Security Centre (NCSC) Minimum Cyber Security Standard and relevant codes of connection. • ICT Asset management system in place. • Log monitoring system in place that supports Information Security. • Improved patching process. • Annual health checks undertaken, and action plans being delivered. • Change management processes in place. • New firewalls and VPN installed. • Regular monitoring of cyber threats. • Cyber/Data Incident response plan in place. • Information governance impact assessment arrangements in place to ensure privacy by design approach and that appropriate technical security controls are in place for new or changed systems and processes. • Information related activity complies to current legislation and regulations including the Data Protection Act, 	<ul style="list-style-type: none"> • Responding to industry best practice and legislative requirements to ensure the security of our infrastructure and data assets. • Alignment with the NCSC Minimum Cyber Standards. • Increased security focused culture. • Fully embedded ICT governance. • Assurance that all third-party systems and hardware meet our integration requirements. • Using log monitoring proactively to support service improvements. • Making full use of the security options within Office 365. • More resilient end point and mail protection in place. 	<ul style="list-style-type: none"> • Establish standardisation for hardware and software to provide increased assurance on compliance regardless of where developed.  Support and develop fit-for-purpose software systems (in house and externally purchased) that meet the needs of the Service.  Centrally manage all end user hardware devices online to assure security updates and patching is applied consistently reducing the risks to the service infrastructure. • Review our Mobile Device Management and Log Monitoring systems to ensure we make best use of resources and the new technologies available.  Assure our firewalls are continually fit-for-purpose, meeting the ESN code of connection requirements, as well as being sustainable to support online partnership working. • Simplify password management whilst still maintaining high levels of security • Continue to raise awareness and train our staff in information security.
	<h3 data-bbox="786 1029 1406 1074">Where we will be in five years</h3> <ul style="list-style-type: none"> • Ability to use any hardware device to securely access our network. • Increased ability to access and share information in a live incident field through fixed vehicle or mobile hardware. • An infrastructure and associated processes that protect the Service's 	

<p>General Data Protection Regulation, Security Policy Framework, Freedom of Information Act and the Human Rights Act and changes are monitored.</p>	<p>information in an increased threat environment.</p> <ul style="list-style-type: none">• Whole Service one team proactive approach to ICT security.	<ul style="list-style-type: none">• Replace end point protection and implement Office 365 mail protection.
--	---	--

Operational Communications


With a focus on  Equality, Diversity & Inclusion and  Environmental Sustainability

Where we are now	Where we will be in three years	What we will do
<ul style="list-style-type: none"> • Creation of an Operational Comms and Control department to deliver an integrated approach to operational communications incorporating ESN implementation, end user requirements, ICT developments and the next generation Control system. • Deployment of new hardware and continuous improvements in functionality of Operational Communications on the incident ground. • Realisation of savings from and future proofing of devices through effective cross departmental working. • Utilising ESN as data bearer for station end mobilisation thereby removing key PSTN action. • Reviewing and replacing station end equipment. • Maintaining Officer Mobile devices ahead of ESN replacement programme. 	<ul style="list-style-type: none"> • Implemented findings for Flexi Duty Officer technology review in line with ESN developments. • Transitioned to ESN phase 1 with risk information tablets having full data access through ESN sims. • Implemented a single ESN compliant Officer device. • In final stages to implement the new command and control system. • Delivered the engagement and communication strategy to all affected staff and programmed the works needed to move service control centre to new central location. • ESN transition preparations completed. • Implemented use of appliance handheld ESN devices. • Provided secure access to the DWFRS network for data over ESN. • Improved business continuity plan through effective integration of communication systems across the Service. 	<ul style="list-style-type: none"> • Develop use of MDT (Mobile Data Terminals) technology, exploring and implementing additional capability and functionality to assist personnel. • In line with the Emergency Services Mobile Communication Programme, transition from Airwave to ESN for all critical operational communications. • Develop and implement new technology for risk management as part of a wider Fire Risk Management project. • Work closely with fleet and equipment to ensure future technical capabilities form part of specification, procurement and delivery of new appliances. • Offer improvements for flexi duty officer's ways of working through integrated devices and software. • Support delivery of new command and control system. • Identify opportunities to deliver value for money while matching organisational needs.

<ul style="list-style-type: none"> • Identifying opportunities for efficiencies through improved electronic accessibility on the incident ground through mobile and removable devices e.g., command forms, incident ground management software. • Reviewing future technology requirements for flexi duty officers to improve ways of working. • Working closely with Cyber Security and Information Management and ICT Teams to maintain the Emergency Services Network Code of Connection. • Direct Network Service Provider Managed Firewall installed with live data services. • An early adopter for ESN Connect services and mobilising station-based appliances over ESN. • Working with other data service providers to enable use over the ESN network. • ESN Network Assurance work underway. 	<ul style="list-style-type: none"> • Integrated operational communications strategy utilising the priority and pre-emption offered by the ESN network. 	
<p style="text-align: center;">Where we will be in five years</p>		
	<ul style="list-style-type: none"> • Full transitioned to ESN secure network with devices provisioned and linked to enable smarter and more resilient working • Control will have moved to new location in line with the Asset strategy. • Newly contracted command and control system in place and embedded • Integrated risk information, operational communication and incident command part of a networked solution available at all operational incidents. 	




ICT Resilience

With a focus on  Equality, Diversity & Inclusion and  Environmental Sustainability

Where we are now	Where we will be in 3 years	What we will do
<ul style="list-style-type: none"> • Highly resilient, geographically separated data centres. • High-speed link between data centres. • Fallback facility from one to another should an area fail. • Disk-based backup with geographically dispersed storage. • Reliable and resilient connectivity to Partner sites to support Networked Fire Control. • All servers virtualised. • System monitoring in place. • Highly resilient connectivity to the Internet with automatic fail-over. • New back-up system in place. • Wi-Fi upgrade rolled out. 	<ul style="list-style-type: none"> • Server hardware reviewed and updated. • Storage reviewed and updated to match Service requirements. • Systems in place to assist in operational availability and capacity planning. • Backup system that can be re-sized for the changes that will take place as more data moves into Cloud Services. 	<ul style="list-style-type: none"> •  Update the distributed Server Farm and investigate benefits of hybrid and/or cloud delivery of the server farm for future proofing. • Ensure the OS (Microsoft Data Centre 2012) is fit-for purpose, review these products at the same time the servers are replaced/upgraded for sustainability. • Distributed data storage system (linked to distributed server farm activity above) to be reviewed and replaced where appropriate including reviewing the on-going storage requirements to ensure that the current Service needs and new ways of working are met. • Review Mutiny firewall software alongside other monitoring systems in place to against business requirements to ensure right tools are in place, vulnerability gaps are closed no overlaps and or duplication across systems to assure value for money.
	<h3 data-bbox="786 722 1406 762">Where we will be in five years</h3> <ul style="list-style-type: none"> • Automated recording systems in place providing analysis and business intel to support proactive ways of working to continually increase resilience. • Fit for purpose storage and monitoring systems that meet the future state business and environmental needs. 	

Technology Management

With a focus on  Equality, Diversity & Inclusion and  Environmental Sustainability

Where we are now	Where we will be in three years	What we will do
<ul style="list-style-type: none"> • Fully networked and managed printer environment with all printing costs understood and accounted for. • Realistic cost-effective replacement programs based on business need. • Alerter base stations that support phased alerting. • Airwave radio system installed. • Fireground radio replacement programme underway. • Mobile data devices in use for data collection. • MDTs (Mobile Data Terminals) installed in appliances. • Increased use of RITs (Risk Information Tablets) functionality for different business activities. • Use of dash cameras and body worn cameras. 	<ul style="list-style-type: none"> • End-user devices that match the requirement of a role. • Integration of software systems. • Clear path for infrastructure upgrades. • Clear path for the provision of secure corporate mobile devices. • Implementation of the ESMCP and ESN national project. • High-speed data connectivity to the fireground. • MDTs utilised to collect data at incident. • Move to a single communications device for Officers. • Implementation of new telephony across the service in line with smarter working and making best use of technology. • New ways of alerting officers to incidents. 	<ul style="list-style-type: none">  Review the replacement programme annually in line with the smarter ways of working agenda to ensure that users have the right hardware to meet the needs of the service and their role. • Review the new telephony needs across the service and deliver a new solution to improve efficiency, reliance and reduce costs. • Station Uninterruptible Power Supply (UPS) replacements will be undertaken based upon age and battery life predictions. Full replacement expected in 2025 with a move to a consistent make and model across all stations to ensure ease of maintenance. • Replacement of Multitone station end equipment replacing the operating system to maintain security.  More efficient processes and technology to manage business requirements of this hardware.  Support the Service in identifying how technology can support delivery of training and align this vision to capital and project development programmes.
	<h3 data-bbox="786 1058 1406 1106">Where we will be in five years</h3> <ul style="list-style-type: none"> • Continued environmental scanning and development of technology to meet the needs of the Service. • Review and expanding ESN functionality. 	

Digital Transformation

With a focus on  Equality, Diversity & Inclusion and  Environmental Sustainability

Where we are now	Where we will be in three years	What we will do
<ul style="list-style-type: none"> • Digital Transformation Programme Board monitoring the delivery of the four workstreams: <ul style="list-style-type: none"> ○ Two-year document migration programme from file shares to SharePoint ○ Notes systems into Office 365 ○ HRMIS review ○ Process improvements using tools in Office 365 • Office 365 and Teams in full use for meetings across the whole Service. • Direct remote access available for all users with Service devices. • Full Wi-Fi coverage at all service locations. • Guest and staff guest Wi-Fi access available at all Service locations. • 1Gb bandwidth to the Internet. • Implementation of Voice over Internet Protocol (VoIP) at all Service locations. • Wi-Fi delivered to all Service locations, but no guaranteed full-site coverage. 	<ul style="list-style-type: none"> • Full Service migration from file shares to Office 365. • Key systems developed into Office 365 from Lotus Notes. • Implementing the recommendations of the HRMIS and process review. • All Service locations to be connected by either direct fibre or fibre to the cabinet. • Cloud based management of Wi-Fi systems. • All Service locations to have sufficient bandwidth to support video delivery as a minimum. • Seamless authentication and Single Sign-On where possible. • Wide use of the systems and tools available from Office 365 to align with our smarter working principles. • Document collaboration being the norm. • Improved records management and information security. <p>Where we will be in five years</p> <ul style="list-style-type: none"> • All service users to be confident in using Office 365 tools. • Utilising Office 365 for most of our systems and processes. 	<ul style="list-style-type: none"> • Deliver the digital transformation programme workstreams: <ul style="list-style-type: none"> ○ Document migration programme from file shares to SharePoint. ○ Notes systems into Office 365 ○ HRMIS review ○ Process improvements using tools in office 365 • Adopt a Cloud first approach wherever possible when procuring new systems and software to reduce infrastructure costs. • Maintain and develop specialist skills in line with technological changes. • Provide training and support to end users to facilitate the cultural changes associated with embracing new technology and smarter ways of working.  Review bandwidth against business needs and increased remote access requirements, as well as accounting for change to web based and cloud ways of working. • Improve authentication and implement single sign-on to as many

<ul style="list-style-type: none"> • All service users with access to cloud-based calendars and mail (O365). • All service users with access to cloud-based file storage and sharing (O365). • Records management within SharePoint, Teams and file servers. • Dedicated team delivering digital transformation. • Some paper records that need management within SharePoint, Teams and file servers. • A mixture of hosted and locally managed third-party systems. 	<ul style="list-style-type: none"> • Internal Technology first approach 'what is already in use that we can adapt' i.e.O365. • Digital by default fully embedded. • Self-service O365 functionality set across the business to develop as per departmental needs within a service wide parameter. • Linked processes regardless of originating software or data recording point. • All third-party systems to be within a hosted environment. 	<p>applications as possible to improve efficiency and security.</p>
--	--	---

Business Intelligence and Data Management

With a focus on  Equality, Diversity & Inclusion and  Environmental Sustainability

Where we are now	Where we will be in three years	What we will do
<ul style="list-style-type: none"> • Corporate management of key information systems. • Effective management of data quality and retention in legacy systems. • Corporate data informing strategic decision making to mitigate risk and improve service delivery. • Use of dashboards to inform local risk management at station and departmental level and for Fire Authority scrutiny. • Linking prevention, protection and response through effective data management. • The majority of KPIs and performance measures configured with automatic data feeds. • High-level automated information available within our corporate Geographical Information System (GIS). • Data and information are a critical resource assisting with planning, mobilising and organising, leading and controlling an incident. 	<ul style="list-style-type: none"> • Assurance that all third-party systems and hardware meet our integration requirements in terms of data management. • Ensuring data consistency throughout the Service to provide a single version of the truth. • Data retention established and managed across all systems. • Information Asset Owners proactively managing data quality. • Service wide use of corporate data via dashboards using PowerBi. • Further integration of data and systems to enhance the information and intelligence available to teams and departments. 	<ul style="list-style-type: none"> • Continued use of PowerBi and Office 365 tools to integrate data and provide client focused useable front end. • Migration of corporate systems to hosted environments. • Establish clear data retention processes for all corporate systems. • Review approach to mapping in terms of Service benefits and NFSP collaborative working.
	<h3>Where we will be in five years</h3> <ul style="list-style-type: none"> • Data management at the forefront of all business process and system development and change. • GIS to be at the forefront of the intelligence data being supplied to help inform all business decisions. 	

Glossary

ADSL	Asymmetric Digital Subscriber Line. Technology that will offer faster connection speeds than the traditional Internet via dial-up telephone lines could offer.
App	An abbreviation for "application" A piece of software that comes pre-installed on your device, or software that you install yourself. Apps typically run locally on your device but can also run through a web browser.
Band Width	The maximum amount of data transmitted over an internet connection in a given amount of time. Bandwidth is often mistaken for internet speed when it is actually the volume of information that can be sent over a connection in a measured amount of time – calculated in megabits per second (Mbps).
BAU	Business as usual.
Cloud Based	A term that refers to applications, services or resources made available to users on demand via the Internet from cloud computing providers' servers. It is important to note <i>the servers to manage the data still exist</i> , just not on your own site, therefore you do not hold responsibility for their upgrading, management, and speed of accessibility.
ESMCP	Emergency Services Mobile Communication Programme. Home Office-led Emergency Services Mobile Communications Programme (ESMCP) is a cross-departmental programme set up to develop/deliver new communications to replace the current Airwave system. The new service will be called the Emergency Services Network (ESN).
ESN	Emergency Service Network. Transmits fast, safe and secure voice, video, and data across the 4G network and give first responders immediate access to life-saving data, images and information in live situations and emergencies on the frontline.

Firewall	A network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
HMICFRS	Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services. Independently assesses the effectiveness and efficiency of police forces and fire & rescue services – in the public interest.
ICT	Information & Communication Technology. An electronic medium for creating, storing, manipulating, receiving, and sending information from one place to another, including the internet, wireless networks, phones, computers, software, middleware, infrastructure, security, video, social networking, and bespoke applications and services.
KLOE	Key Lines of Enquiry. These identify where we are, where we need to go and the things, we need to deliver.
MPLS	Multi-Protocol Label Switching. Data forwarding technology that increases the speed and controls the flow of network traffic.
NFCSP	Networked Fire Control Services Partnership. A partnership established to provide a collaborative approach to the future provision of fire control services across the region, which covers a population in excess of five million. The partnership is between Devon & Somerset, Dorset & Wiltshire, and Hampshire & Isle of Wight.
NFSP	Networked Fire Services Partnership. A partnership between ourselves and Hampshire & Isle of Wight and Devon & Somerset fire and rescue services. This partnership works to achieve a more joined up approach to our emergency response and to save money across the three Services.
Office 365 / Microsoft 365	Includes applications like Word, Excel, PowerPoint, and brings together other productivity apps with powerful cloud services, device management, and advanced security in one experience. Microsoft 365 is the higher-level package of services which includes Office 365 , alongside other business tools. A user can subscribe to Office 365 without also subscribing to Microsoft 365 - but all Microsoft 365 users will also have access to Office 365.
PowerBi	A Microsoft business analytics service that provides interactive visualisations and business intelligence capabilities via dashboards.

PSTN	Public Switched Telephone Network. A telecommunications network which allows subscribers at different sites to communicate by voice i.e. traditional telephone service.
Strategic Assessment of Risk	To ensure that the Community Safety Plan remains current and reflective of the landscape within which the Service operates, a Strategic Assessment of Risk (SAR) is undertaken. The SAR directs the focus of the Service and is the starting point of the corporate planning cycle. It draws on a broad range of information, data, intelligence, risks, and threats to set out the high-level factors that will impact on the Service's operating environment. The SAR is then used to ensure that the priorities within the CSP remain focussed, maximising the impact the organisation has on improving public safety and health and wellbeing.
VoIP	Voice over Internet Protocol. Also called IP telephony is a method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol networks, such as the internet.
VPN	Virtual Private Network. Protects identity and browsing activity from hackers, businesses, government agencies, and other snoops. When connecting to the internet, data and IP address are hidden by a type of virtual tunnel. This keeps others from seeing the online activity.
Wi-Fi	Wireless Fidelity. The technology that allows a PC, laptop, mobile phone, or tablet device to connect at high speed to the internet without the need for a physical wired connection.