MERSEYSIDE
FIRE & RESCUE
SERVICE

Data & Technology - ICT Asset Management Plan

2024 - 2029

Table of Contents

Data & Technology - ICT Asset Management Plan

1 Overview

1.1 Data and Technology (D&T) Department

The D&T Department is responsible for Information and Communications Technology (ICT) asset management. As a result, the Head of D&T, the D&T Service Delivery Team and the Applications & Technology (A&T) Team has the primary responsibility for ICT asset management.

A key element is to proactively manage the existing outsourced ICT managed service contract with its ICT partner, Telent. We work in partnership to ensure the maintenance of vital '999' emergency response infrastructure, as well as continuing to expand the use of ICT technology to manage our resources efficiently and effectively in line with the risks facing the communities of Merseyside and our firefighters and the organisational processes of the Authority.

1.2 Asset Ownership & Responsibilities

The Authority currently owns the ICT assets in the ICT infrastructure and the ICT applications that run on the ICT infrastructure. The ICT challenge is to provide the most secure, functional, flexible ICT infrastructure possible and to host the applications that deliver benefits to the Authority, all at the lowest cost of ownership. Meeting this challenge systematically through having the right people in the right structure, Infrastructure Lifecycle Management (ILM), Application Lifecycle Management (ALM) and best practices, such as the ITIL, can lead to improvements in efficiency, performance, and cost management.

ICT can be split into six key delivery area:

- The ICT infrastructure: data, voice and radio networks, personal computers (PCs) and devices, servers, printers, etc
- Commodity applications which run on the ICT infrastructure: Structured Query Language (SQL), Oracle, Microsoft Office and O365
- Fire Control applications which run on the ICT infrastructure: Vision 5 Computer Aided Dispatch (CAD), Vision 5 BOSS, Airbus ScResponse
- Corporate applications that run on the ICT infrastructure: Tranman, Planning Intelligence and Performance System (PIPS), the intranet ‘Portal’ (SharePoint) and CFRMIS
- Financial and HR applications which run on the ICT infrastructure: ABS eFinancials, ResourceLink and the Staff Attendance Recording System (StARS)
- The ICT Service Desk: The central point of contact between ICT providers and users on a day-to-day basis. It is also a focal point for reporting *incidents* (disruptions or potential disruptions in service availability or quality) and for users making *service requests* (routine requests for services)

ICT ILM and ALM is carried out by D&T and Telent on behalf of the Authority; it is done so in line with best practice from the ITIL framework. ITIL is a set of best practices and processes for the management and delivery of ICT services and support.

The processes are mature, providing an infrastructure that is robust, secure, reliable and resilient, and applications that are secure, efficient and effective in meeting the needs of the organisation, and provide benefits to the communities of Merseyside.

Note, Finance and People and Organisational Development (POD) are directly responsible for their own applications, however, they are aligned to D&T governance.

1.2 ICT Asset Management

ICT asset management is carried out by the D&T department on behalf of the Authority and it is done so in line with ITIL and Information Technology Asset Management (ITAM). The terminology 'ITAM' is interchangeable with ICT Asset Management.

In line with the organisation's policy for asset management, the lifecycle of an ICT asset has four distinct phases:

- Planning
- Acquisition
- Operation
- Disposal

And ICT follows five major principles:

- ICT asset management decisions are integrated with the strategic planning process
- ICT asset planning decisions are based on an evaluation of the alternatives, which consider the 'lifecycle' costs, benefits and risks of ownership
- Accountability is established for ICT asset condition, use and performance
- Effective disposal decisions are carried out in line with minimal environment impact
- An effective control structure is established for ICT asset management

Further information on how D&T manages ICT assets on behalf of the Authority can be found in the remainder of this plan.

Return to Top.

2 ICT Asset Management Strategy

ITIL ITAM is the set of business practices that join financial, contractual and inventory functions to support lifecycle management and strategic decision-making for the ICT environment. ICT assets include all elements of software and hardware that are found in the organisation's environment.

Under ITAM, D&T manages its assets effectively to help deliver its strategic priorities and services in line with risk; providing value-for-money-services for the benefit of the local community.

D&T has all of its ICT assets recorded in a Configuration Management System (CMS) and the Definitive Media Library (DML). 'Remedy' records details of all the ICT assets and their age, thus enabling D&T to effectively manage the lifecycle of its infrastructure. It gives the ability to link ICT incidents, assets and people, to enable a more in-depth trend analysis to be performed around ITAM decisions.

D&T has a service catalogue, which outlines all the ICT services provided. Included in this catalogue are references to the capacity planning, security and preventative maintenance carried out on ICT assets.

D&T has a robust reporting process to provide systematic and timely reporting of compliance and performance, enabling prompt asset-related decision-making regarding ICT assets.

D&T has a service pipeline. The service pipeline comprises new ICT services under development, and these developments lead to new, or a change of use of, ICT assets (see Section 5 D&T Service Pipeline for further details).

To manage the ICT five-year capital asset investment plan, D&T classifies spend into four categories:

- Underlying Spend
- ICT Project Spend
- Community Risk Management Plan (CRMP) Project Spend (previously the Integrated Risk Management Plan)
- Fire and Rescue Service (FRS) National Project Spend

D&T has a five-year lifecycle-renewal policy for ICT hardware assets such as personal computers, devices and servers, at which point these assets will be considered end-of-life (EOL).

D&T has a 5-10-year lifecycle-renewal policy for ICT hardware assets such as network switches and telephony, at which point these assets will be considered EOL.

When an ICT asset is highlighted as EOL, its performance is assessed and, if required, a new asset will be purchased.

Adopting a best practice, asset management and configuration management solution allows D&T to understand:

- What ICT assets the Authority has
- Where they are located
- How well they are working
- How effectively they are supporting the business of the organisation

As a result, the following benefits have been realised:

- Accurate information on all ICT assets, providing D&T with the ability to deliver and support its services
- Trend analysis can be carried out against assets to aid incident and problem-solving
- Improved security through advanced ICT asset control
- Improved financial planning through clear identification of all assets and their associated relationships
- Improved software licence management, ensuring legal compliance
- Increased confidence in ICT systems and D&T services
- Increased customer satisfaction

A snapshot-in-time list of the Authority's hardware ICT assets can be found in Appendix A – Summary of ICT Infrastructure Assets. This list can be requested and produced from Remedy to give a real-time view of the ICT asset holding. On a yearly basis, the list is produced for insurance calculation purposes.

The system is also used for various analytical tasks including:

- Identification of obsolete ICT assets, based on purchase date
- Identification of current and previous ICT asset owners
- ICT asset rationalisation
- Role Based Resourcing (RBR)

All ICT assets pass through a configuration management process where they are allocated and labelled with a unique asset reference number.

In line with ITIL, D&T has a DML to improve the way it tracks software and performs ALM.

Return to Top.

3 ICT Infrastructure Asset Monitoring Activities

D&T maintains an up-to-date service catalogue which outlines all the services provided. Included in this catalogue are references to capacity planning, security and preventative maintenance, all of which are examples of activities carried out on ICT assets.

3.1 Capacity Planning

'Capacity planning is used to ensure that the Authority has adequate capacity to meet its demands, even during periods of extreme high usage and growth. This includes, but is not exclusive to, estimation of disk space, computer hardware, software and network infrastructure that will be required over a set amount of time.'

Capacity is calculated in various ways depending on the system and specific requirements from D&T.

Regular storage reports are run on servers and file shares, which are used for current and projected growth estimations using bespoke software.

Additionally, network management software is utilised to manage the capacity of all network links used within the Authority's Wide Area Network (WAN) and Local Area Network (LAN).

3.2 Security

'The Authority requires multiple levels of security on managed devices to defend against malicious behaviour and mitigate the risk to the Authority.'

Patching is one of the most important parts of a cyber-security strategy; keeping things on the latest version, in most cases, means greater security.

Merseyside Fire and Rescue Authority (MFRA) has a patching policy in place and it applies to each area of the ICT infrastructure. Patching is conducted based on the assessment of risk. This policy is prudent; balancing the need to reduce the amount of downtime to critical systems with cyber-security risk.

The introduction of Microsoft System Centre Configuration Manger (SCCM) has seen patching carried out over and above Business as Usual (BAU) activity, because of the ability to automate tasks.

To assist in the automation of processes and administration of the status of both end point devices and servers, an ICT infrastructure discovery tool – Nexthink – has been deployed to enable the ICT estate to be tightly managed and, importantly, easily reported on.

This provides security by design, audit and assurance; Nexthink highlights hardware and software, if it is not fully patched and up to date, to allow MFRA to adhere to the required patching level defined by the Airwave Code of Connection (CoCo).

A key response to cyber-security is Security Information and Event Management (SIEM) and MFRA has implemented LogPoint as a SIEM tool. This ensures that the appropriate levels of security information are both readily available and stored for an agreed length of time.

Forcepoint is used to protect end-user devices from spam, viruses and other malicious threats via e-mail and internet. The solution configuration is hybrid hosted and on-premises. Sophos Endpoint Protection is used to secure the Authority's systems – including, but not limited to, Windows servers, Windows desktops, Surface Pros and mobile devices – against viruses, malware, advanced threats and targeted attacks.

Mobile Device Management (MDM) for Samsung mobiles phones is in place, along with appliance Toughpads, protecting our information more securely than in the past.

MDM is provided by Sophos Mobile Control and Microsoft Intune; providing a full suite of management and security tools for any device, covering the important capabilities of management, security, productivity and compliance.

With the introduction of UK General Data Protection Regulation (GDPR) and Data Protection Act (DPA), in addition to the ever-changing security threats from mobile malware and data loss, blue light organisations and partner agencies have realised that they require effective MDM to complement existing security protocols.

Devices containing potential sensitive data are encrypted up to 256 bits using Advanced Encryption Standard (AES).

3.3 Device Preventative Maintenance

'Telent is responsible for device preventative maintenance, including planned maintenance activity designed to improve equipment life and avoid any unplanned maintenance activity.'

The Authority requires desktops and laptops to be configured with Sophos Anti-Virus and Windows Updates via a Windows Server Update Services (WSUS) Server.

Windows critical updates are installed via the WSUS server, and recommended updates are reviewed and tested before installing on end-user devices.

Recently, SCCM has been introduced. SCCM is a systems management software product developed by Microsoft for maintaining large groups of computers running Windows 10.

Sophos performs a full daily scan on each device and alerts via desktop and e-mail alerting if any issues are reported.

BIOS/firmware patching is performed when a device is re-imaged from the software library or if a specific fault occurs.

3.4 Audit

In 2021/2022, internal audit focused on the audit area of 'MFRA Asset Management of ICT Devices and Phones'. The audit objective was to review the arrangements in place at MFRA for management of ICT devices and phones, to obtain assurance on the adequacy and effectiveness of the controls.

The scope of the audit included examining controls relating to the following areas:

- Accuracy of the ICT asset register.
- That there is a nominated officer responsible for maintaining the ICT asset register.
- That new stock is added to the asset register on receipt.
- That there is an effective strategy for refreshing obsolete equipment.
- That obsolete stock is disposed of in line with industry standards, and the asset register updated.
- That assets allocated to staff who leave are returned to ICT, 'wiped' and reused where appropriate and the asset register updated.

An action tracker in response to findings of the internal audit, published in 2023, has been created and is presented at the quarterly meetings of the Strategy & Performance (S&P) D&T Board, where remedial activities are discussed, monitored and approved.

Return to Top.

4 ICT Infrastructure Asset Monitoring Reports

Effective ICT asset management requires a monitoring process to provide systematic and timely reporting of compliance and performance, to enable prompt asset-related decision-making. D&T prepares and publishes the following reports to fulfil this function:

4.1 Service Desk Performance Report – Monthly

The monthly ICT Service Desk Performance Report is provided to enable Telent, D&T and the Authority's officers to review the service delivery of ICT for the Authority and, if required, any escalation can be taken to the Strategy and Performance D&T Board.

4.2 ICT Infrastructure Usage Report – Monthly

The monthly ICT Infrastructure Usage Report is provided to enable Telent, D&T and the Authority's officers to review and discuss infrastructure usage, review the top 10 users of each asset and share the information with the Authority's budget holders.

4.3 Information Security Report – Monthly

The monthly Information Security Report provides Telent, D&T and the Authority's officers (including the Senior Information Risk Owner [SIRO]) with relevant information that supports the Authority's information security policy. It is posted on the Portal and is reviewed at the Protective Security Group (PSG) Meeting.

4.4 Problem Management Reports – Monthly

In line with ITIL service management processes, this report provides the statistical analysis and evidence that supports problem management.

Problem management seeks to proactively minimise incidents by identifying and recording problems and known errors within the ICT infrastructure. Errors within ICT infrastructure can cause repeated incidents, which have an adverse effect on the business. Identifying and removing errors can reduce the number of incidents over time.

4.5 Major Incident Management Reports – Ad Hoc

Whenever a major ICT Incident takes place, a Major Incident Management Report (MIR) is produced and reviewed with a view to establishing lessons learnt and to feed back into the ICT service catalogue.

Return to Top.

5 D&T Service Pipeline

The service pipeline comprises new D&T services under development, and these developments lead to new, or a change of use of, ICT assets. D&T has seven main areas associated with the service pipeline:

- ICT Service Requests
- D&T Cyber Security & Information Management
- D&T Continuous Service Improvement (CSI)
- Application & Technology Lifecycle Management
- D&T Strategic Framework
- Strategy and Performance D&T Board
- Other ITIL Standards

A full list of key D&T projects can be found in Appendix B – Key D&T Projects and Activities.

5.1 ICT Service Requests

The ICT Service Desk Digital Workplace allows users to report issues and incidents as well as requesting simple technical changes, information, enquiries or hardware and software changes, e.g. mobile phones.

For certain ICT requests, an approval route through the D&T Service Delivery Manager is needed. The ICT request process is fully integrated in the CMS, with all changes being documented.

5.2 D&T Cyber Security & Information Management

Reporting to the Head of Data & Technology; the Cyber Security & Information Management Manager will coordinate the Service's approach to cyber-security, business intelligence and information management and governance. The role will develop the Service's strategy for cyber-security: advising on the suitability of the design; tools; activities; control measures and processes, required to mitigate cyber-security risks in relation to the Service's applications and technology technical architecture (current and proposed).

5.3 D&T Continuous Service Improvement (CSI)

The purpose of the D&T CSI meeting is to ensure that cost-justifiable ICT capacity in all areas of ICT exists and is matched to the current and future agreed needs of the business in a timely manner. A key focus is on increasing the efficiency, maximising the effectiveness and optimising the cost of services and the underlying ICT service management. Meetings follow a six-week cycle and the process is documented in the CSI register. This CSI process is now firmly embedded in the D&T department, and the key benefits are:

- Clarity of ownership
- Clarity of requirements
- Clarity and management of costs
- Visibility and tracking progress

- Forward planning
- Resource scheduling
- Identifying duplicate effort across the Authority's departments and/or stations
- The ability to utilise information from archives

5.4 Lifecycle Management

The D&T challenge is to provide the most functional, flexible ICT infrastructure possible and to host the applications that deliver benefits to the organisation, all at the lowest cost of ownership. Meeting this challenge systematically through having the right people in the right structure, ILM, ALM and best practices such as ITIL can lead to improvements in efficiency, performance and cost management.

5.4.1 ILM

ILM encompasses the planning, design, acquisition, implementation and management of all the elements comprising the ICT infrastructure.

5.4.2 ALM

ALM encompasses the planning, design, acquisition, implementation and management of all the elements comprising the application portfolios.

5.4.3 ITIL

ITIL is a globally accepted approach and set of practices for IT Service Management (ITSM) that focuses on aligning ICT services with the needs of the business.

5.5 D&T Strategic Framework

The D&T Strategic Framework is a cycle of four meetings that takes place on an annual basis and the output feeds into the quarterly S&P D&T Board.

The D&T Strategic Framework is part of the governance applied to the delivery of the Telent ICT managed service; meetings are held once a quarter to cover one of three topics. There are two 'Innovation and Technology Forums', an 'Efficiency and Value for Money Meeting' and a 'Strategy and Alignment Meeting' held each year.

The D&T Strategic Framework ensures that the ICT managed services contract:

- Is working effectively
- Has its strategic goals set by, and aligned with, the needs of the Authority
- Improves efficiency of arrangements and delivers mutually beneficial savings and efficiencies

5.6 Strategy and Performance (S&P) D&T Board

There are three thematic S&P boards in place: D&T, Estates, and Performance, which means a thematic S&P D&T Board meets every three months. The purpose of the S&P D&T Board is to ensure that all data and technology services are aligned to ensure the mission and objectives of the Authority are delivered as effectively as possible.

5.7 Other ITIL Standards

- A Change Advisory Board (CAB) has been set up which will ensure that only authorised changes are deployed to the Authority's infrastructure. This will also improve the communication between key system owners and D&T

- D&T maintains and develops a DML. It ensures that:

    - A secure compound is established in which master copies of all authorised versions of the organisation's software are stored and protected

    - All documents pertaining to applications are stored in a central location, e.g. number of users, location of users, contact details of suppliers and Service Level Agreements (SLAs)

- D&T sets minimum release management standards which third party suppliers are expected and contracted to reach

Return to Top.

6 D&T Infrastructure Asset Replacement Policy

D&T has in place procedures to trace the acquisition, deployment, management and disposal of ICT assets under its control.

Some of the primary goals for asset replacement are:

- To develop an appropriate type of replacement mix based on each asset and its behaviour
- To ensure value for money
- To meet the desired/acceptable level of risk
- To enable realistic forecasts of future events

6.1 ICT Asset Purchasing

In the main, the Authority owns the ICT assets. When ICT assets are purchased by D&T, the following applies:

- For small quantities of ICT commodity assets, the Authority's ICT outsourced partner will seek quotes and the Authority will purchase
- For large quantities of ICT commodity assets, the Authority's ICT outsourced partner will specify requirements, but the Authority's procurement team will run mini-competitions and the Authority will purchase
- For ICT assets which require complex installation or if priority support is required; the Authority's outsourced partner specifies and purchases the item on the Authority's behalf and then the Authority pays via change control
- In such cases, the Authority's ICT outsourced partner is requested to run a mini-competition and produce options for the Authority to select
- Purchasing is done via the contract change control procedure, and the Change Control Note (CCN) is signed off by D&T, Procurement and Legal. No mark-up is charged by the Authority's ICT outsourced partner, as the contract makes provision for commercial services

6.2 ICT Asset Disposal

D&T has in place procedures for the disposal of ICT assets via a company called ‘Computer Waste’. Computer Waste is an Authorised Treatment Facility (ATF), fully registered by the Environment Agency (EA). The company specialises in the recycling of waste electrical and electronic equipment (see WEEE).

- All ICT assets disposed of with Computer Waste are recorded on a waste transfer note that is signed and presented to the Authority for audit purposes

- Hard drives are destroyed on the Authority premises, witnessed by an employee of Telent, and an accompanying destruction certificate is presented to the Authority for audit purposes

6.3 ICT Hardware Assets

D&T has a five-year lifecycle-renewal policy for ICT hardware assets such as PCs, tablets, mobile devices and servers, at which point ICT Assets will be considered end-of-life, if there are confirmed performance issues. A three-year equipment life was considered but the increased capital spend was deemed to be excessive.

Furthermore, the proliferation of devices along the wide spectrum of ICT presents opportunities and challenges to D&T, as well as budget challenges to the organisation. There is a policy of using shared MFDs and having one MFD per function, to replace printers. This printer rationalisation has contributed to budget savings.

RBR is undertaken by D&T, evaluating the agile provision of ICT equipment at stations, SHQ, Training and Development Academy (TDA), Vesty One and ‘incidents’, based on the roles of the staff housed or present there.

An Asset Based Resourcing (ABR) initiative is also in place as a check and balance to RBR, ensuring operational vehicle assets match the role of firefighters and senior officers who use such vehicles.

D&T has a 5-10-year lifecycle-renewal policy for ICT hardware assets such as network switches and telephony, at which point ICT assets will be considered end-of-life, if there are confirmed performance issues.

ICT assets could also be replaced on an ad-hoc basis, but this would lead to difficult budget forecasting, with some years seeing larger budget increases than others. If, however, ITIL problem management analysis identifies an ICT hardware asset that is repeatedly problematic, causing a break in service, the equipment would be considered for replacement before its five-year equipment life had expired.

6.4 ICT Asset Movements 2023/2024

Key ICT asset movements to highlight in 2023/2024. Note: these are activities, over and above those in Section Seven - Fire Control Applications and Hardware Assets of this report.

Enhanced Virgin Media Network

A replacement and upgrade of all elements of the Virgin Media Network (Otherwise known as the Wide Area Network (WAN). This major project, involving the upgrade of network equipment across the estate, has been successfully completed. The focus will now turn to the Local Area Network (LAN).

Community Fire Station Audio Visual Replacement

The successful rollout of Clevertouch screens and large TV-like screens to 18 community fire stations. Work is now underway to replace audio visual equipment in the Private Finance Initiative (PFI) stations.

Service Headquarters Conference Audio Visual Replacement

With commercials now in place, it is anticipated that commissioning will be completed by the end of the financial year 2023/24. A further update will follow in next year's asset management plan.

Forcepoint & Sophos

Forcepoint (web filtering) & Sophos (anti-virus) after contract renewal, the completion of the move to using the cloud versions of each product.

Multi-Functional Device (MFD) Implementation

Following a compliant procurement process, HP (Apogee) MFD commissioning and Konica MFD decommissioning. This involved the replacement of approximately 60 MFDs across the whole estate.

Upgrade to Remedy

Telent use the Remedy IT Service Management (ITSM) tool for the Service Desk, asset tracking and other activities. Remedy 9 went live for MFRS, incorporating a new self-service portal.

Telent Contract Extension

The award of a two-year contract extension with Telent Technology Services Ltd, the Authority's ICT outsourced service provider. Telent have undertaken to facilitate the ICT for the new TDA, the new fire station builds, Fire Control technical advancements and ICT continuous service improvement (CSI).

Realigned Capital ICT Budget

Work done to realign the Five-Year ICT Capital budget to deliver the following three large and complex projects:

- Enhanced LAN
- Enhanced audio-visuals (AV)
- ICT server virtualisation and upgrade to SQL 2019

All three project are underway and are expected to be completed early in the financial year 2024/2025.

National Resilience (NR) Audio Visual

Provision of Clevertouch room solution and audio visual in the Area Manager’s office.

Vitavox Long Range Speaker (VLS -LRAD)

The introduction to MFRS via Telent of several battery-powered, high-performance loudspeaker system, designed to transmit warning signals and voice messages over long distances. The use is predominantly for operational incidents involving high rise flats.

Microsoft Enterprise Agreement (EA)

Successful renewal of the Authority’s Microsoft Enterprise Agreement (EA) and, in doing so, awarding of a contract to Phoenix Software Limited to act as the Authority’s Microsoft Licensing Solution Partner (LSP). The contract value with Phoenix is £809k over three years. This includes the cost of Microsoft licences, cloud services and a small margin for Phoenix to act as the Authority’s LSP.

Return to Top.

7 Fire Control Applications and Hardware Assets

Reporting to the Head of Data & Technology, the Applications & Technology Manager works with the Authority's outsourced ICT partner to carry out appropriate lifecycle management to ensure successful ICT service delivery in line with SLAs. Activities include:

- Following of best practice ICT asset management
- Application or infrastructure replacement or refresh
- Spare holding to replace faulty equipment, which is one method in ensuring SLAs are met
- Application Life Cycle Management
- Year-on-year preventative maintenance in mid-October prior to the bonfire period. This is done for both Primary and Secondary Fire Control infrastructure and applications
- Regular relocation exercises to Secondary Fire Control

7.1 Six High Level Areas of ICT in Fire Control.

There are six high level areas of ICT in Fire Control.

- **Computer Aided Dispatch (CAD)** - This is where incoming emergency calls are logged, and the appropriate resources mobilised to the incidents. MFRA uses the SSS (formally Capita) Vision 5 CAD application, implemented in April 2021.

- **Management Information System (MIS):** providing senior officers with real time incident information and the organisation with incident history for trend analysis. MFRA use the SSS Vision 5 BOSS.

- **An Integrated Communications Control System (ICCS)** - an ICCS is found at the centre of modern-day control rooms. All communications that go into the control room such as 999 and administration telephony calls, radio communication and CCTV are routed via the ICCS. The control room staff can then manage these various communication channels from one place on their desktop by accessing the ICCS.

  An ICCS will work in tandem with a CAD application. The ICCS is the place where incoming emergency calls are answered, and the CAD is where the calls are logged and resources dispatched. MFRA use the SSS Ds3000 ICCS.

- **Wide Area Radio Scheme:** Emergency services rely on seamless radio communications coverage to effectively perform their daily tasks. MFRA, in keeping with the Police and Ambulance, use Airwave.

NOTE: The Emergency Services Mobile Communication Programme, (ESMCP) set up by the Home Office, aims to replace the current communication service provided by Airwave. The new service will be delivered across the Emergency Services Network (ESN) and MFRA will connect to this network via a Direct Network Service Provider (DNSP). As at February 2024, however, all individual FRS activities for this project remain suspended.

- **Data Mobilisation:** Fire Control can mobilise crews to incidents by sending a message to the Mobile Data Terminal (MDT) installed in the appliance. MFRA use MDTs running ScResponse from Airbus.

- **Station-End Turnout**: Various hardware and software components and subsystems are installed in every MFRS community fire station. The solution involves automatically unlocking doors; switching on of lights; sounding the alarm and printing the emergency turnout information on the fire station printer. This enables crews to respond to emergency turnouts in a safe and efficient manner. MFRA utilise station-end Firecoders from Multitone Electronics.

7.2 Fire Control ICT Project Review

CAD-MIS is a series of projects where D&T has delivered, and will continue to deliver, improvements for Fire Control.

CAD-MIS Phase One

CAD-MIS Phase One: In September 2017, the Authority approved a project to replace Vision 3 FX CAD & Vision 3 MIS with applications supplied by NEC SWS.

The implementation of Vision 5 went live on 21st April 2021 and a period of early life support followed. Vision 5 assists in our duty to respond to all emergency calls with a level of response appropriate to the risk, and deal with all emergencies efficiently and effectively.

CAD-MIS Phase Two

Following successful completion of Phase One activities, a prioritised list of Phase Two activities was finalised and approved. What follows is an update on the activities chosen:

- **Dispatch Communication Server (DCS) -** The technical refresh element of this activity has been completed and a working DCS connection has been established. Fire Control has completed User Acceptance Testing (UAT). Following the IT Health Check of the DCS connection, a Remedial Action Plan (RAP) was submitted to the accreditor and was subsequently approved. A monthly report of progress with the RAP is now in place with the accreditor. This is deemed to be a successful completed project.

- **Dynamic Cover Tool –** Geographical display of availability of appliances, highlighting areas of under- and over-resourcing. Following an issue with the drawing of isochrones in some areas in Merseyside, the development team has been working on a new version which uses an alternate road network and isochrone tool (OpenStreetMap and GraphHopper). Both are open-source products that will give us more control of the changes that are made. The new version has been released to Fire Control for testing.

- **Fire Survival Guide –** An internal solution has been produced and implemented into Fire Control, and this satisfies minimum requirements.

CAD-MIS Phase Three

Mindful of the requirement to maintain the appropriate lifecycle management of hardware and software applications, a series of related phase three activities commenced in 2023/2024.

- **Enhanced Mobilisation:** The budget for this project was approved at the Policy and Resources Committee on 14th December 2023. A next stage review meeting took place with NEC SWS (formally SSS) and the project has moved to NEC SWS creating a user story and providing class two pricing.

- **Fire Control Refurbishment:** w/c 12th February 2024 is the final week of the five-week refurbishment. The media wall and the Fire Control workstations, including new screens and standing desks adaptations will take place.

- **ResponseEye (999Eye)**: Situational awareness for call handlers. Budget for this activity has been moved to the financial year 2025/2026.

Post CAD-MIS Phase Three

Following CAD-MIS Phase Three, the Authority will be in a strong position to take stock and assess the introduction of the next generation of Fire Control Command & Control solutions.

This requirement has been identified within the Five-Year ICT Capital Plan Commentary stating that the existing Vision 5 and the DS3000 ICCS will need replacing circa 2028/2029 at an estimated cost of £2m and that work on a separate business case is recommended to commence in 2024-2025.

7.3 Emergency Services Network (ESN)

Following the early departure of Motorola from the ESMCP programme in December 2022, the Home Office have commenced a re-procurement exercise for a replacement Lot 2 supplier/Prime Contractor.

The Home Office therefore suspended all ESN related activities from March 2023 for a period of 12–18 months or until such time that the re-procurement exercise completes.

ESMCP Assurance Partner activities that MFRS was involved in ceased after March 2023 and the Home Office have thanked MFRS for the work and effort undertaken in testing the associated products and delivering many of the key project milestones.

The consequences of the ESN suspension are that whilst the DS3000 technical refresh and DCS Install projects will continue and complete during 2023, the ESN Solution Deployment project will terminate with immediate effect.

Return to Top.

8 ICT Commodity Application Software

D&T is responsible for ensuring the Authority has an ALM strategy for all its commodity applications. D&T works closely with all departments to develop and manage organisational commodity applications and agree and monitor SLAs.

8.1 Microsoft Software: Enterprise Agreement (EA)

The Authority's strategic direction is to use Microsoft products.

To continue to use the latest versions of Microsoft products, such as Window Server, Windows 10, Windows 11 and O365, MFRA has a Microsoft Enterprise Agreement (EA) for the majority of its Microsoft software licences.

In 2023/2024 the MFRS Microsoft EA was renewed under the Crown Commercial Services (CCS) Digital Transformation Arrangement 2021 (DTA21).

The DTA21 runs until April 2024, and it is a Memorandum of Understanding (MOU) between the UK Government and Microsoft to enable public sector organisations to continue to unlock the benefits of cloud computing and business applications.

Under the EA, Microsoft has bundled together Windows, Office 365 and a variety of management tools to create a subscription suite: Microsoft 365 (M365). MFRA is licensed for M365 and this has allowed D&T to deploy Microsoft Teams together with other M365 products.

At the same time as the renewal, MFRS awarded a three-year contact to a Microsoft LSP. A LSP provides information and guidance about contacting, identifying and choosing Microsoft licensing.

8.2 Anti-Virus and E-mail Filtering

The anti-virus software, Sophos, protects the Authority from computer viruses and any other threats which may try to enter the Authority's network.

The e-mail filtering system, Forcepoint, is used to filter e-mail and quarantine non-legitimate e-mails via the process of word detection. The words that result in the email being quarantined are recorded in a database and analysed on a monthly basis.

The licences for the anti-virus and e-mail filtering products are procured on a three to five year lifecycle and, prior to any future renewal, a fit-for-purpose exercise and market evaluation will be carried out.

Return to Top.

9. Corporate and Financial Application Software

9.1 Application Classification

Applications are managed through their lifecycle in collaboration with application owners and are given a classification to identify their status. The classifications include:

New	Conceived, in planning phase, under construction or newly deployed
Emerging	In production or licences have been purchased, but in limited use, such as a pilot
Mainstream	In production and actively being used
Containment	In production for a specific or limited purpose
Sunset	In production with scheduled retirement in progress
Prohibited	No longer used

See Appendix D – Application Status for a full list of applications.

9.2 Application Requests

Any department with a requirement for a new or replacement application must, in the first instance, complete the Application Request Form. The form can be accessed from the S&P homepage on the Portal. The form captures the following information:

- Identified application sponsor and owner
- Organisational need/value
- Risks to the organisation
- Legislative requirements
- Potential efficiency savings
- Collaboration considerations
- Budget allocated for this application

If the application request is approved for progression to the next stage, a further business case is required, detailing the market engagement carried out, cost benefit analysis and recommendations.

9.3 Application Gateway Team

The purpose of the Application Gateway Team is to provide the Authority with effective governance arrangements for new or replacement applications. The Application Gateway Team is responsible for approving and prioritising the advancement of new or replacement applications within the organisation. See Appendix D – Application Status for a full list of applications.

9.4 Application Development

9.4.1 Application Toolkit

The Application Development Team utilises a suite of products that assists with the development of internal applications:

Azure DevOps	Azure DevOps is a Microsoft product that provides version control, reporting, requirements management, project management, automated builds, lab management, testing and release management capabilities. It covers the entire application lifecycle and enables DevOps capabilities.
Azure IaaS	Infrastructure as a service (IaaS) provides a secure and scalable infrastructure.
Azure SaaS	Software as a service (SaaS) allows users to connect to and use cloud-based apps over the Internet.
Visual Studio	Microsoft Visual Studio is an integrated development environment. It is used to develop computer programs, as well as websites, web apps, web services and mobile apps.
ReSharper	ReSharper is a popular developer productivity extension for Microsoft Visual Studio. It automates coding routines by finding compiler errors, runtime errors, redundancies, etc.

9.4.2 DevOps

DevOps is the union of people, processes and products to enable continuous delivery of value to our end users. The combination of ‘Dev’ and ‘Ops’ refers to avoiding siloed ‘Development’ and ‘Operations’ by using multidisciplinary teams that work together with shared and efficient practices and tools. DevOps has been adopted as a recognised framework to ensure the success of any app development and to align developed apps and infrastructure; Dev being the Application Development Team, Ops being ICT/Telent, both of which are part of the D&T department.

9.4.3 Development Portfolio

The application development portfolio currently consists of the following applications.

Application	Classification
OPS (Operational Performance System)	Sunset
SSRI Progress	Sunset
National Resilience Application	Mainstream
Merseyside Fire & Rescue Service Website	Mainstream
AURA	New

9.5 Financial Implications of New or Replacement Applications

The requirement for new or replacement applications is monitored throughout the year and will follow the application governance process outlined in sections 9.2 and 9.3 of this document.

There will be two large scale application projects undertaken during this five-year period, and capital reserves have been identified and put in place to support these projects. The Finance, HR & Payroll, and Procurement applications (FHRPP) and Time and Resource Management applications are due for replacement within the next two years and an additional £100K capital has been set aside.

In addition to the above, there has been budget allocated in the ICT capital programme to fund other applications that are planned for the next five years.

The application portfolio will be kept under review and requests for additional capital or revenue will be submitted if required. It is not envisaged that they will be significant amounts.

Return to Top.

10 ICT Asset Capital Spend Strategy

10.1 ICT Asset Investment Process

To manage the ICT asset investment process, D&T classifies spend into four categories:

- Underlying Spend
- ICT Project Spend
- CRMP Project Spend
- National FRS Project Spend

These are explained in the following table:

	Spend	Why	Benefit
Underlying Spend	Spend on the existing ICT infrastructure including software, devices, servers, networks and voice communication e.g. upgrade of station switches.	This spend stops the ICT infrastructure and any software becoming out of date.	More than just 'keeping the lights on'. An ICT-enabled organisation whose systems are robust, secure and resilient, with the ability to accommodate change.
ICT Project Spend	Projects that: deliver Authority changes, deliver step changes in technology e.g. MDT evolution.	This spend delivers value for money, innovation and savings, where appropriate.	ICT accommodating change with a focus on a sound business case and clear deliverables.
CRMP Project Spend	Spend on specific IRMP/CRMP projects where ICT is a major enabler e.g. station change.	This spend delivers the Authority's CRMP.	To be the best Fire & Rescue Service in the UK. One team, putting its communities first. Releasing budget for frontline resources.
National FRS Project Spend	Spend on specific national projects where ICT is a major enabler e.g. ESMCP.	Spend to align the Authority's systems to national initiatives.	Protecting public safety and increasing national resilience.

The 2024/2029 Five-Year Capital Plan can be found in Appendix C – 2024/2029 ICT Five Year Capital Plan

10.2 Review of the Current Capital Programme

D&T carries out an annual full review of its capital budget. The basis for the review is to:

- Determine if any reductions in planned spend was possible, and/or
- Determine if the asset life could be reviewed (extended) to reduce the frequency of replacing assets etc. and/or
- Determine if anything else could be done to reduce the level of planned borrowing and therefore reduce the impact of debt servicing costs on the future revenue budget.

This asset management plan has been updated to reflect this review.

10.3 The Emergence of Cloud Computing

The D&T cloud strategy is:

‘Application development in the public cloud to transform existing processes to meet business needs, whilst exploring the public cloud, hybrid cloud and on-premises, to deliver dynamically automated ICT infrastructure management, the promise of reduced costs and the ability to run mission-critical applications.’

The move to the cloud and taking ICT as a service, rather than buying a product and installing it on ICT equipment, moves the cost of ICT from being mostly a capital, one-off cost, to an on-going revenue cost. Therefore, investment in ICT over the coming years will not be a case of deciding where to spend the capital budget, but instead one of choosing between spending revenue on ICT systems or on other priorities.

D&T will work closely with Finance to achieve this transition over the coming years.

Return to Top.

11 Glossary

ABR	Asset Based Resourcing
AES	Advanced Encryption Standard
ALM	Application Lifecycle Management
AP	Assurance Partner
ATF	Authorised Treatment Facility
AV	Audio visual
BAU	Business as Usual
BIOS	Basic Input/Output System
BRM	Business Relationship Management or Manager
CAB	Change Advisory Board
CAD	Computer Aided Dispatch
CCN	Change Control Note
CCS	Crown Commercial Service
CFRMIS	Community Fire Risk Management Information System
CMS	Configuration Management System
CoCo	Code of Connection
CRMP	Community Risk Management Plan
CSI	Continuous Service Improvement
CTA	Cloud Transformation Agreement
D&T	Data & Technology
DCS	Dispatch Communications Server
DML	Definitive Media Library (previously Definitive Software Library, DSL)
DNSP	Direct Network Service Provider
DPA	Data Protection Act
DTA	Digital Transformation Arrangement
ED&I	Equality, Diversity and Inclusion
EA	Enterprise Agreement *or* Environment Agency
EOL	End-of-life
ESMCP	Emergency Services Mobile Communications Programme
ESN	Emergency Services Network
FDS	Functional Design Specification
FRS	Fire and Rescue Service
GPS	Global Positioning System
GDPR	General Data Protection Regulation
IAAS	Infrastructure as a Service
ICCS	Integrated Communications Control System
ICT	Information and Communication Technology
ILM	Infrastructure Lifecycle Management
IM	Information Management
IRMP	Integrated Risk Management Plan
ITAM	IT (or ICT) Asset Management
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management

LAN	Local Area Network
LFB	London Fire Brigade
LSP	Licensing Solution Partner
MDM	Mobile Device Management
MDT	Mobile Data Terminal
MFD	Multi-Function Device
MFRA	Merseyside Fire and Rescue Authority
MIR	Major Incident Report
MIS	Management Information System
MOU	Memorandum of Understanding
OPS	Operational Performance System *or* short form for Operations
PC	Personal Computer
PIPS	Planning Intelligence and Performance System
PM	Project Manager
PSG	Protective Security Group
RAP	Remedial Action Plan
RBR	Role Based Resourcing
S&P	Strategy and Performance
SAAS	Software as a Service
SAN	Storage Area Network
SCCM	System Centre Configuration Manager
SIEM	Security Information and Event Management
SIRO	Senior Information Risk Owner
SLA	Service Level Agreement
SMS	Service Management System
SOFSA	Simple Operational Fire Safety Assessment
SQL	Structured Query Language
StARS	Staff Attendance Recording System
TDA	Training and Development Academy
WAN	Wide Area Network
WEEE	Waste Electrical and Electronic Equipment
WSUS	Windows Server Update Service

Return to Top.

Appendix A – Summary of ICT Infrastructure Assets

Fire Control Services and Infrastructure	Quantity
CAD Servers – Tier 1 (≤£5000)	17
CAD Servers – Tier 2 (≥£5000)	0
CAD Desktops	32
CAD Monitors	52
ICCS Servers	1
ICCS Clients	20
ICCS Touchscreen	20
ICCS Capita VAIU	0
Fire Control Headsets	40
Airwave SAN H Radio Gateway	1
Alerter Masts	4
UHF Radio Packsets	632
Station End Firecoders	27
Station End Turnout Printers	32
Station End Auxiliary Relay Unit (ARU)	32
Station End Amplifiers	34
Station End UPS	40
Modems	63
Mobile Data Terminals	43
Airwave Radio SAN A	112
Airwave Radio SAN B	10
Airwave Radio SAN J	80

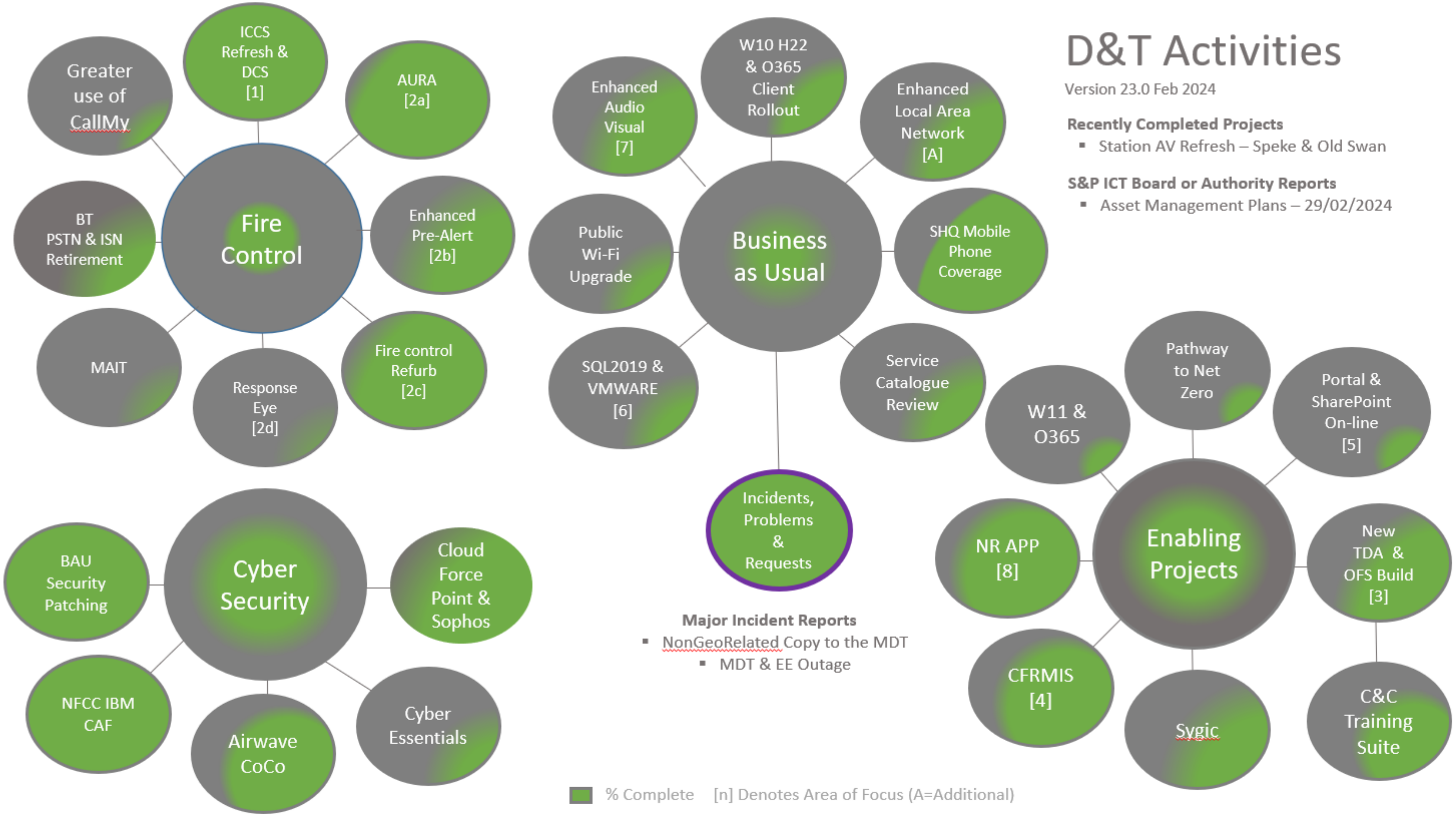
Administration Infrastructure, Managed Servers, Desktop, and mobile devices	Quantity
Servers – Tier 1 (≤£5000)	39
Servers – Tier 2 (≥£5000)	3
HPE Modular Storage Arrays (MSA)	3
HPE Storage Shelves	8
HPE Tape Library	1
Desktops	318
Laptops	20
Microsoft Surface Pro	374
Microsoft Surface Laptop	123
Microsoft Surface Book	14
Microsoft Surface Go	14
Panasonic Toughpads	101
Docking Stations (Laptops & Surface Devices)	649
Docking Stations (Toughpads)	186
Monitors	1187

Non-Standard Printers (not Apogee devices)	9
Konica Minolta Multi-Function Devices	53
Konica Minolta Desktop Print Devices	10
Security Appliance – Tier 1 (≤£2000)	5
Security Appliance – Tier 2 (≥£2000)	5
Router – Tier 1 (≤£2000)	10
Router – Tier 2 (≥£2000)	26
Switch – Tier 1 (≤£2000)	31
Switch – Tier 2 (≥£2000)	56
Wireless Controller	1
Wireless Access Points	90
Mitel IP Sets	674
Mitel Conference Unit	12
Ubiquiti Nanobeam Wireless Bridge	2
SIKLU Radio Link	6

Mobile phones, Smartphones and **Miscellaneous**	**Quantity**
Smartphones (Samsung)	432
iPhones	12
Non-Smartphones (Alcatel/Nokia)	453
MTPAS Enabled Mobile SIMS	104
MDT Enabled Data SIMS	42
iPads	13
Encrypted USB devices	138
3G/4G Dongles	33
Battery Chargers	137
Projectors (includes Smartboards)	29
Barco Click Share	11
Display Screens	35
Clevertouch Screen	16
IPTV - Gateways	1
IPTV - Receivers	30
Remote Access Tokens (Celestix)	169
Running Call Phones	24

Return to Top.

Appendix B – Key D&T Projects and Activities



D&T Activities

Version 23.0 Feb 2024

Recently Completed Projects

- Station AV Refresh – Speke & Old Swan

S&P ICT Board or Authority Reports

- Asset Management Plans – 29/02/2024

Fire Control

- Greater use of CallMy
- ICCS Refresh & DCS [1]
- AURA [2a]
- Enhanced Pre-Alert [2b]
- Fire control Refurb [2c]
- Response Eye [2d]
- MAIT
- BT PSTN & ISN Retirement

Business as Usual

- Enhanced Audio Visual [7]
- W10 H22 & O365 Client Rollout
- Enhanced Local Area Network [A]
- SHQ Mobile Phone Coverage
- Service Catalogue Review
- Incidents, Problems & Requests
- SQL2019 & VMWARE [6]
- Public Wi-Fi Upgrade

Cyber Security

- BAU Security Patching
- Cloud Force Point & Sophos
- Cyber Essentials
- Airwave CoCo
- NFCC IBM CAF

Major Incident Reports

- NonGeoRelated Copy to the MDT
- MDT & EE Outage

Enabling Projects

- W11 & O365
- Pathway to Net Zero
- Portal & SharePoint On-line [5]
- New TDA & OFS Build [3]
- C&C Training Suite
- Sygic
- CFRMIS [4]
- NR APP [8]

🟩 % Complete [n] Denotes Area of Focus (A=Additional)

Highlighted Business as Usual (BAU)

Item	Description	Status
Incidents, Problems & Requests	These are the day-to-day disruptions to the ICT BAU Services. e.g. loss of internet, e-mail.	Major Incidents since last board: (i) NonGeoRelated Copy to the MDT – awaiting report (ii) MDT & EE Outage – Agenda item
Enhanced Local Area Network (LAN)	This project involves: - (a) Replacement of Wireless Access Points - (b) SHQ User Stack Switches Replacement - (c) Core Network Switches Replacement	This is the first the three large, complex and significant ICT infrastructure projects. Orders have been placed and kit has been delivered. Current activities include (1) SHQ User access switches have been replaced (2) SHQ inter rack fibre is in place (3) Cisco Core network switches installation and bench testing is underway.
SQL 2019 & VMWARE	New Server virtualisation, backup solution and upgrade to on-premise SQL 2019.	The ICT server virtualisation will provide the platform on which SQL 2019 will reside. Hardware has been delivered and Telent is liaising with the supplier, HPE, which has been engaged to commission and install the hardware solution.
SHQ Mobile Phone Coverage	Senior Officers have highlighted issues with O2 coverage in the Conference Room corridor and Joint Control Centre (JCC) Silver Command.	The install of the Office of Communications (Ofcom) approved O2 Cell Fi Quatra was put on hold. Senior Officers are currently using Wi-Fi calling.
Windows 10 & O365	Upgrade to Windows 1022 H2 and upgrade Microsoft Office to the O365 version.	These upgrades are different from upgrades done in the past as they need to be user-initiated. This has been completed for Telent and ICT and no training issues have been identified. Rollout of W1022 H2 & O365 to the Change Advisory Board (CAB) is underway.
Windows 11	Windows 11 is the latest major release of Microsoft's Windows NT operating system. It will only work on devices which satisfy the new Windows 11 system requirements.	Telent will use Nexthink, a network discovery tool, to determine the scale of the ask and formulate a migration plan. This will begin in the fiscal year 2024/25.

Highlighted Projects

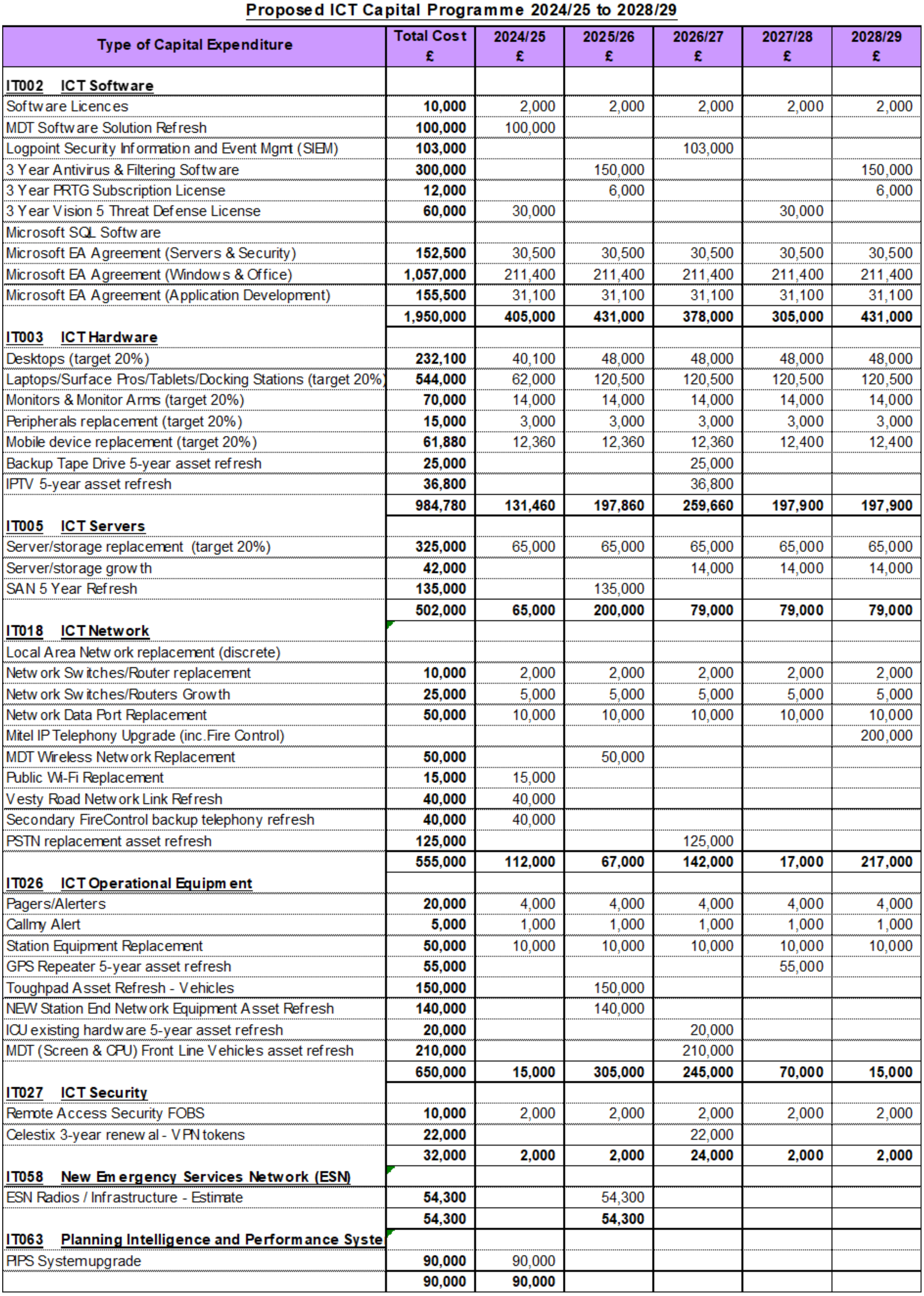
Item	Description	Status
Enhanced Audio Visual	This project involves: - Station Audio Visual - SHQ Audio Visual - Fire Control Media Wall & OSR Audio Visual	(i) SHQ AV: Order has been raised. Installation dates to be finalised once lead times have been confirmed. (ii) Media Wall & OSR: Orders have been raised. Installation dates to be finalised once lead times have been confirmed. (ii)Station AV: Rollout complete. Speke & Old Swan completed since last meeting.
Sygic	Integrated into the MDT, Sygic Sat Nav has premium quality maps and auto-routing to location on receipt of incident details.	The initial trial of Sygic on M14P1 (Speke) was well received by crews. Speke will be a early adopter as Sygic is rolled out with an 64-bit build update.
Cyber Essentials	Cyber Essentials is a simple but effective, government-backed scheme that helps to protect organisations, whatever their size, against a range of the most common cyber attacks.	This activity has been restarted following a pause as ICT participated in the NFCC Cyber Resilience Assessment of Fire and Rescue Services (FRS) in England.
BT PSTN & ISDN Retirement	In 2025 the last elements of Openreach's analogue and digital ISDN copper network will be turned off as an all-IP network replaces these legacy services. The impact on telephony and broadband services is far-reaching and it will affect the 999s.	1. Following a BT Survey. Orders to BT/Openreach around SIP telephony, including the 999, for the New TDA and replacing the ELSA divert with Smart numbers have been placed. 2. The Cradle Point solution for secondary mobilisation to Station has been selected and order has been placed for the New Aintree Station. 3. LFB, Surrey and Yorkshire FRS are testing SIP for their 999s. A watching brief is being maintained.
Long Lane New TDA	New TDA & OFS main build, Secondary Fire Control lift & shift, and the new immersive Command & Control Training Suite.	The Telent PM is on-board, & continues to work with Fire Control for the move of Secondary Fire Control. (i) Following the Telent Change Control Note (CCN) process, key orders have been placed. The TDA AV order will be placed in the coming weeks. (ii) Piranha has done the first fix for the C&C Training suite.

Emerging Projects

Item	Description	Status
MAIT	NFCC have secured a £1.34 million section 31 grant from the Home Office for the initial costs in providing both the Multi Agency Incident Transfer (MAIT) Hub and licencing costs for each FRS to connect to the hub for up to three years.	This item was taken to the Operations Board 10th January 2024 along with a letter from Jim Powell, NFCC MAIT Project Executive, providing assurances around funding. The project has been signed off and MFRS will be an early adopter. (i) MFRS will now enter in to a four year contractual agreement with AVR Group Ltd with some. (ii) Fire Control has appointed its MFRS MAIT champion and initial trials of the web based offering is underway. (ii) Telent is currently discussing connectivity to the MAIT HUB with its supplier.

Return to Top.

Appendix C 2024/25 – 2028/2029 ICT Five Year Capital Plan

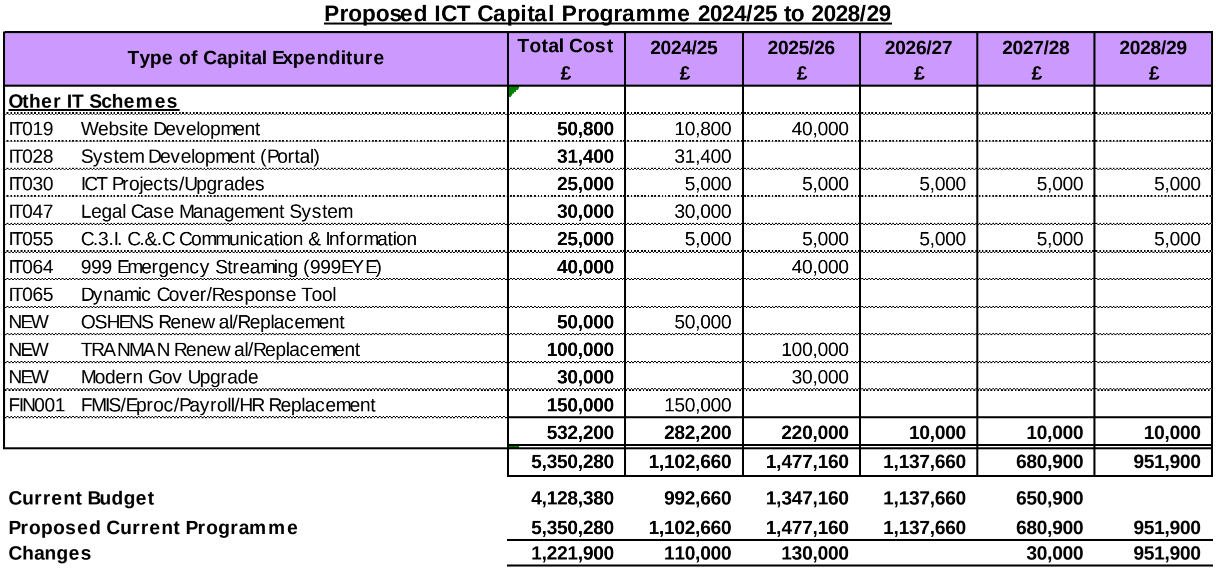


Proposed ICT Capital Programme 2024/25 to 2028/29

Type of Capital Expenditure	Total Cost £	2024/25 £	2025/26 £	2026/27 £	2027/28 £	2028/29 £
IT002 ICT Software						
Software Licences	**10,000**	2,000	2,000	2,000	2,000	2,000
MDT Software Solution Refresh	**100,000**	100,000				
Logpoint Security Information and Event Mgmt (SIEM)	**103,000**			103,000		
3 Year Antivirus & Filtering Software	**300,000**		150,000			150,000
3 Year PRTG Subscription License	**12,000**		6,000			6,000
3 Year Vision 5 Threat Defense License	**60,000**	30,000			30,000	
Microsoft SQL Software						
Microsoft EA Agreement (Servers & Security)	**152,500**	30,500	30,500	30,500	30,500	30,500
Microsoft EA Agreement (Windows & Office)	**1,057,000**	211,400	211,400	211,400	211,400	211,400
Microsoft EA Agreement (Application Development)	**155,500**	31,100	31,100	31,100	31,100	31,100
	1,950,000	**405,000**	**431,000**	**378,000**	**305,000**	**431,000**
IT003 ICT Hardware						
Desktops (target 20%)	**232,100**	40,100	48,000	48,000	48,000	48,000
Laptops/Surface Pros/Tablets/Docking Stations (target 20%)	**544,000**	62,000	120,500	120,500	120,500	120,500
Monitors & Monitor Arms (target 20%)	**70,000**	14,000	14,000	14,000	14,000	14,000
Peripherals replacement (target 20%)	**15,000**	3,000	3,000	3,000	3,000	3,000
Mobile device replacement (target 20%)	**61,880**	12,360	12,360	12,360	12,400	12,400
Backup Tape Drive 5-year asset refresh	**25,000**			25,000		
IPTV 5-year asset refresh	**36,800**			36,800		
	984,780	**131,460**	**197,860**	**259,660**	**197,900**	**197,900**
IT005 ICT Servers						
Server/storage replacement (target 20%)	**325,000**	65,000	65,000	65,000	65,000	65,000
Server/storage growth	**42,000**			14,000	14,000	14,000
SAN 5 Year Refresh	**135,000**		135,000			
	502,000	**65,000**	**200,000**	**79,000**	**79,000**	**79,000**
IT018 ICT Network						
Local Area Network replacement (discrete)						
Network Switches/Router replacement	**10,000**	2,000	2,000	2,000	2,000	2,000
Network Switches/Routers Growth	**25,000**	5,000	5,000	5,000	5,000	5,000
Network Data Port Replacement	**50,000**	10,000	10,000	10,000	10,000	10,000
Mitel IP Telephony Upgrade (inc.Fire Control)						200,000
MDT Wireless Network Replacement	**50,000**		50,000			
Public Wi-Fi Replacement	**15,000**	15,000				
Vesty Road Network Link Refresh	**40,000**	40,000				
Secondary FireControl backup telephony refresh	**40,000**	40,000				
PSTN replacement asset refresh	**125,000**			125,000		
	555,000	**112,000**	**67,000**	**142,000**	**17,000**	**217,000**
IT026 ICT Operational Equipment						
Pagers/Alerters	**20,000**	4,000	4,000	4,000	4,000	4,000
Callmy Alert	**5,000**	1,000	1,000	1,000	1,000	1,000
Station Equipment Replacement	**50,000**	10,000	10,000	10,000	10,000	10,000
GPS Repeater 5-year asset refresh	**55,000**				55,000	
Toughpad Asset Refresh - Vehicles	**150,000**		150,000			
NEW Station End Network Equipment Asset Refresh	**140,000**		140,000			
ICU existing hardware 5-year asset refresh	**20,000**			20,000		
MDT (Screen & CPU) Front Line Vehicles asset refresh	**210,000**			210,000		
	650,000	**15,000**	**305,000**	**245,000**	**70,000**	**15,000**
IT027 ICT Security						
Remote Access Security FOBS	**10,000**	2,000	2,000	2,000	2,000	2,000
Celestix 3-year renewal - VPN tokens	**22,000**			22,000		
	32,000	**2,000**	**2,000**	**24,000**	**2,000**	**2,000**
IT058 New Emergency Services Network (ESN)						
ESN Radios / Infrastructure - Estimate	**54,300**		54,300			
	54,300		**54,300**			
IT063 Planning Intelligence and Performance Syste						
PIPS System upgrade	**90,000**	90,000				
	90,000	**90,000**				

Continued Next Page.

Appendix C 2024/25 – 2028/2029 ICT Five Year Capital Plan - Continued



Proposed ICT Capital Programme 2024/25 to 2028/29

Type of Capital Expenditure	Total Cost £	2024/25 £	2025/26 £	2026/27 £	2027/28 £	2028/29 £
Other IT Schemes						
IT019 Website Development	**50,800**	10,800	40,000			
IT028 System Development (Portal)	**31,400**	31,400				
IT030 ICT Projects/Upgrades	**25,000**	5,000	5,000	5,000	5,000	5,000
IT047 Legal Case Management System	**30,000**	30,000				
IT055 C.3.I. C.&.C Communication & Information	**25,000**	5,000	5,000	5,000	5,000	5,000
IT064 999 Emergency Streaming (999EYE)	**40,000**		40,000			
IT065 Dynamic Cover/Response Tool						
NEW OSHENS Renewal/Replacement	**50,000**	50,000				
NEW TRANMAN Renewal/Replacement	**100,000**		100,000			
NEW Modern Gov Upgrade	**30,000**		30,000			
FIN001 FMIS/Eproc/Payroll/HR Replacement	**150,000**	150,000				
	532,200	**282,200**	**220,000**	**10,000**	**10,000**	**10,000**
	5,350,280	**1,102,660**	**1,477,160**	**1,137,660**	**680,900**	**951,900**
Current Budget	**4,128,380**	**992,660**	**1,347,160**	**1,137,660**	**650,900**	
Proposed Current Programme	**5,350,280**	**1,102,660**	**1,477,160**	**1,137,660**	**680,900**	**951,900**
Changes	**1,221,900**	**110,000**	**130,000**		**30,000**	**951,900**

Return to Top.

Appendix D – Application Status

Merseyside Fire and Rescue Authority - Applications Status Update

ITIL Standards

New	Conceived, in planning phase, under construction or newly deployed
Emerging	In production or licenses have been purchased, but in limited use, such as a pilot
Mainstream	In production and actively being used
Containment	In production for a specific or limited purpose
Sunset	In production with scheduled retirement in progress
Prohibited	No longer used

Application Name	Function	Status
Goldmine (Front Range)	This is a CRM application used by Fire Service Direct in the Community Fire Safety arena.	Prohibited
HFSC App (SharePoint Portal)	InfoPath form used by stations to record and refer home fire safety checks.	Prohibited
IIT Database	Used by IIT to record and report on data relating to incident investigations.	Mainstream
SOFSA (Simple Operational Fire Safety Assessment)	This is used by Protection Department and Stations for recordings information relating to a Simple Operational Fire Safety assessment.	Prohibited
Business Objects	A reporting tool used in Finance.	Mainstream
E-Financials & E-Procurement	Finance, stores and procurement package.	Mainstream

Iken Legal Case Management	Legal case management system includes a library of documents and workflows linked to a central database. Multiple operations and bulk processing are driven from a single input, whilst shared items can be used to store information related to a particular client, matter/case work.	Mainstream
Civica Modern Gov	Committee decisions management system used to manage authority business including ensuring relevant papers are published to members via the MFRA web page.	Mainstream
Resourcelink	NGA HR and payroll functionality hosted by ABS 365 to manage the entire employee lifecycle from recruitment to staff development, succession planning and payroll.	Mainstream
Org Plus	Used by People and Organisational Development to produce organisational charts using the data exported from Resourcelink.	Mainstream
File Director	Scans and organises images of paper documents used in People and Organisational Development.	Mainstream
PageTiger	Software that ensures new joiners have all the information they need for a productive onboarding.	Mainstream
Civica Tranman	Vehicle Fleet Management System.	Mainstream
Red Kite	Equipment/asset management system. Used on stations to ensure operational equipment is checked regularly and appropriately maintained.	Mainstream
Airbus Hydra	Water management solution that manages data relating to hydrants.	Mainstream
Draeger	BA (Breathing Apparatus) testing software.	Mainstream
LearnPro (EFS)	eLearning Management Systems provided by eFireService Ltd.	Sunset
XVR Simulation	Virtual reality incident command training software for emergency services.	Mainstream
Auto CAD Architecture	CAD (Computer Aided Design) software.	Mainstream

(Graitec)		
Timewatch PLC – White Space	Training Resource Planner.	Mainstream
SSRI Progress	Captures site specific risk information and presents it to crews via the MDTs.	Sunset
Voyager Fleet	Black box data logger on vehicles.	Mainstream
CAPITA Vision 5	CAD Computer aided dispatch. This system logs all incoming emergency calls and supports the mobilisation of appropriate resources for incident management. Currently in use within Fire Control.	Mainstream
CAPITA DS3000	ICCS (Integrated Communications & Control System) partnered to the Vision FX CAD System. This system enables Fire Control to utilise radio and telephony functions to manage incoming 999 calls and communicate with MFRA resources. Currently in use within Fire Control.	Mainstream
Vision 5 BOSS	Management Information: providing senior officers with real time incident information and the organisation with incident history for trend analysis.	Mainstream
AIRBUS Sc-Response	Data Mobilisation: Fire Control mobilise crews to incidents by sending a message to the Mobile Data Terminal (MDT) installed in the Appliance. Crews retrieve risk related information from the MDT. Currently in use within operational vehicles and Fire Control.	Mainstream
Operational Performance System (OPS)	Internally developed SQL based application to allow the detailed recording, monitoring and assessment of fire fighter competencies against national standards for firefighters.	Sunset

Resilience Direct	A replacement service for the National Resilience Extranet that can be built upon to provide additional innovative ways to enhance multi-agency working.	Mainstream
Airbus Steps	Operational Incident Management package installed on devices on the Authority incident management vehicle.	Prohibited
OSHENS	Health & Safety management information system.	Mainstream
Simul8 - Process Evolution	Fire Incident Response Simulator (FIRS). Fire Incident Analyser (FIA). Facility Location Planner (FLP). Used by Strategy and Performance for operational response planning and modelling.	Mainstream
Ximes	Shift pattern modeller.	Mainstream
StARS	TRM (Time and Resource Management) staffing system.	Mainstream
AVCO Anycoms	Middleware that reduces the requirement for manual input and transfers files securely between local authorities.	Prohibited
Gazetteer	Aligned Assets Gazetteer Application. Corporate gazetteer in use across the Authority to provide standardised address information and UPRN data to corporate systems and users.	Mainstream
Crystal Reports	Reporting tool used in Strategy and Performance.	Mainstream
IRS (CLG)	Incident Recording System which interfaces, extracts data from Vision.	Mainstream
InPhase - Planning, Intelligence and Performance System (PIPs)	System that streamlines and enhances functionality relating to station plans, business intelligence, performance management, GIS plotting, project and risk management.	Mainstream
Silversands – SharePoint Support	SharePoint Portal is used to provide the corporate intranet and central repository for MFRA core data.	Mainstream
MapInfo GIS	MapInfo is a geographical information system used within Strategy and Performance to display and analyse geo-spatial datasets.	Mainstream
Fueltek	Fuel management system.	Mainstream
HR Solutions Hub – Firefighter Sift Tool	Online assessment and sift tool for firefighter recruitment.	Prohibited

ProContract - Proactis	An online Portal for managing the processes around e-tendering and contracts.	Mainstream
National Resilience Management System (inc. ESS)	A management system used by the National Resilience Assurance Team (NRAT) and the National Coordination Centre (FRSNCC).	Mainstream
Civica CFRMIS (Community Fire Risk Management Information System)	An application used to collect and manage information relating to Protection, Prevention and Preparedness. All information will be stored in a single database and shared between the three functions.	Mainstream
Effective Command – K Lamb Associates	The Effective Command™ tool collates data using three different applications: Training, Incident Monitoring and Formal Assessment.	Mainstream
AURA	An application produced by our internal development team that displays real-time locations and response coverage of MFRS appliances.	New
SQEPtech and Cornerstone LMS	Learning Management System.	New

Return to Top.

Return to Top.