Data & Technology - ICT Asset Management Plan

2026/2031

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 Information Technology Infrastructure Library (ITIL), can lead to improvements in efficiency, performance, and cost management. ITIL is a set of best practices and processes for the management and delivery of ICT services and support.

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), Microsoft M365
- Fire Control applications which run on the ICT infrastructure: Computer Aided Dispatch (CAD), MIS, MDT software
- Corporate applications that run on the ICT infrastructure: Transport management, Planning Intelligence and Performance System (PIPS), the intranet ‘Portal’ and operational risk information software
- Financial and HR applications which run on the ICT infrastructure
- 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.

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

1.3 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 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 by highlighting 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).

Email security and web content filtering is used to protect end-user devices from spam, viruses and other malicious threats via e-mail and internet. 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.

The MDM provides a full suite of management and security tools for any device, covering the important capabilities of management, security, productivity and compliance.

Devices 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 Anti-Virus software 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.

SCCM has been introduced and is a systems management software product developed by Microsoft for maintaining large groups of computers.

Anti-virus software 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.

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 list of key D&T projects can be found in Section 8 Digital Transformation Strategy and 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 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 identify the best route to market and the Authority will purchase
- Where the contract permits for ICT assets which require complex installation service 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

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 (vehicle workshops) and ‘incidents’, based on the roles of the staff located 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 2025/2026

Key ICT asset movements to highlight in 2025/2026. Note: these are activities, over and above those in Section Seven - Fire Control Applications and Hardware Assets of this report.

SIP system for Primary Fire Control

In Jan 2027 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. Design work has been completed with final switch over in Q1 2026.

Enhanced Mobilisation

A project that adds additional functionality to the Fire Control CAD (Computer Aided Dispatch) solution and will alert a crew earlier and put them on standby to attend an incident, making the response faster than it is currently.

MAIT (Multi Agency Incident Transfer)

Implementation of MAIT which now allows Fire Control to share electronic incident records with other Fire & Rescue Services.

AURA (Dynamic Cover Tool)

Internal development of AURA providing a geographical display of availability of appliances; highlighting areas of under- and over- resourcing.

New Server Virtualisation and Backup

New Server virtualisation and backup solution is in place together with upgraded corporate SQL server environment.

Migration of Operational Risk Information

Development and implementation of a new solution to capture operational risk information.

Water Management System

Implementation of a new water management solution.

SharePoint Online Migration

Migration of content from on-premises SharePoint, and development of new Power Apps to replace legacy InfoPath forms.

Mobile Device Management Replacement

Migration from legacy MDM solution to new consolidated security suite including the replacement of 300 mobile devices.

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.

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

- **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 works 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.

- **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).

- **Data Mobilisation:** Fire Control can mobilise crews to incidents by sending a message to the Mobile Data Terminal (MDT) installed in the appliance.

- **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.

7.2 Fire Control ICT Project Review

In 2026/27 work will commence to plan a full review of the above six areas of ICT in Fire Control. All hardware, software and support arrangements will be considered and decisions taken on whether to extend, upgrade or replace each element.

7.3 Emergency Services Network (ESN)

The Emergency Services Mobile Communications Programme (ESMCP) aims to deliver an Emergency Services Network (ESN) which will replace the existing Airwave communications network used by the police, fire and rescue, and ambulance services in the UK.

IBM is now the prime contractor for the ESN, delivering 'User Services' which includes the Mission Critical Push to Talk service.

EE has had its 'Mobile Services' contract extended, which now includes the installation of 2000 generators in the most suitable locations across the country in the event of a national power outage.

Samsung's Mission Critical application has successfully completed push-to-talk and push-to-video calls, confirming operational emergency communications functionality.

The strategy for a National Deployment Plan has been established which has three stages – preparation, mobilisation and transition. Within the preparation stage, MFRS readiness assessment activity will start in February 2026, with national transition delivering ESN by Q4 2029.

Return to Top.

8 Digital Transformation Strategy

Our Digital Transformation Vision:
To deliver a more efficient and effective fire and rescue service by leveraging digital technologies that enhance operational capabilities, improve decision-making, optimize resource deployment, and connect the workforce.

Digital Transformation Projects 2026/27:

- Support the implementation of the second phase of the Government’s Fire and Rescue Data Platform (FaRDaP).

- Support the upgrade/replacement of MFRS applications:
  - Health and Safety management
  - Fleet Management
  - Mobile Data Terminal software

- Review the market and consider the most appropriate Incident Command Solution for implementation.

- Develop an application to assist with the management of information requests.

- Develop further enhancements of the National Resilience application, together with the requirements from the ND2 project.

- Continue to develop the Service’s approach to the use and governance of AI technologies.

9 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.

9.1 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 11 and M365, MFRA has a Microsoft Enterprise Agreement (EA) for the majority of its Microsoft software licences.

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.

9.2 Anti-Virus and E-mail Filtering

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

The e-mail filtering system 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.

Return to Top.

10 Corporate and Financial Application Software

10.1 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.

10.2 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.

10.3 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.

10.4 Application Development

10.4.1 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.

10.4.2 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, both of which are part of the D&T department.

10.4.3 Development Portfolio

The application development portfolio currently consists of the following applications.

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

Return to Top.

11 ICT Asset Capital Spend Strategy

11.1 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 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 2026/2031 Five-Year Capital Plan can be found in Appendix C – 2026-2031 ICT Five Year Capital Plan

11.2 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 is 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.

11.3 Cloud Strategy

The D&T cloud strategy is to:

- Continue to develop cloud-based solutions to transform existing and future processes to meet business needs, achieving high levels of resilience and availability.

- Continue to move to cloud-based solutions for new and replacement software applications where organisational benefits can be realised.

- Explore the public and hybrid cloud to deliver dynamically automated ICT infrastructure management.

Return to Top.

12 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
CAB	Change Advisory Board
CAD	Computer Aided Dispatch
CCN	Change Control Note
CCS	Crown Commercial Service
CMS	Configuration Management System
CoCo	Code of Connection
CRMP	Community Risk Management Plan
CSI	Continuous Service Improvement
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
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
ITAM	IT (or ICT) Asset Management
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
LAN	Local Area Network
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
OPS	Operational Performance System
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
SQL	Structured Query Language
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)	19
CAD Desktops	34
CAD Monitors	28
ICCS Servers	6
ICCS Storage (HADS)	1
ICCS Clients	24
ICCS Touchscreen	24
Fire Control Headsets	40
Alerter Masts	7
Station End Firecoders	26
Station End Turnout Printers	30
Station End Auxiliary Relay Unit (ARU)	30
Station End Amplifiers	33
Station End UPS	37
Modems	61
Mobile Data Terminals	61
Airwave Radio SAN A	112
Airwave Radio SAN B	10
Airwave Radio SAN J	81
Media Wall Solution	1
Cradlepoint Solution	26

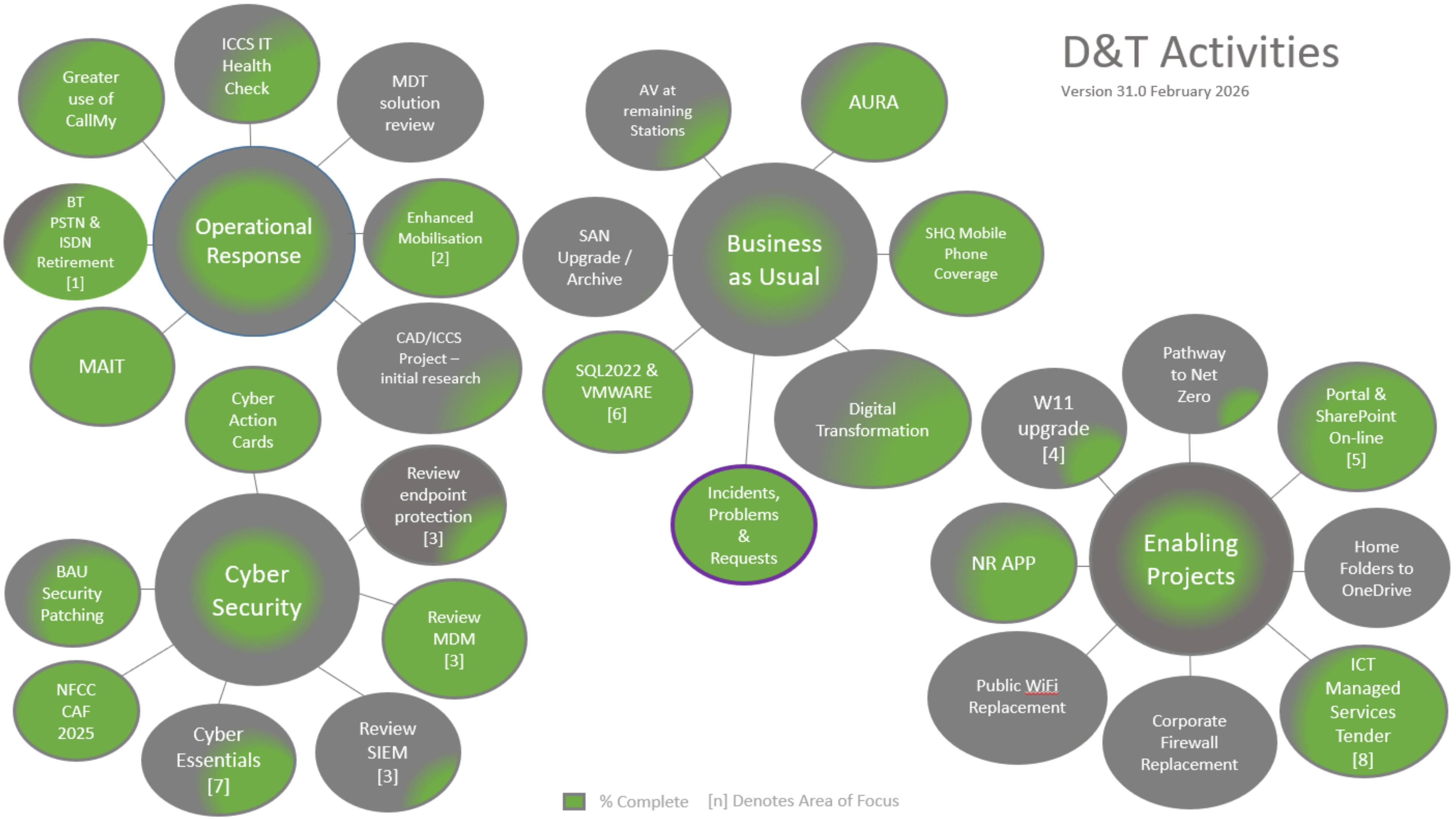
Administration Infrastructure, Managed Servers & Desktop	Quantity
Servers – Tier 1 (≤£5000)	41
Servers – Tier 2 (≥£5000)	3
VM Server Infrastructure (dHCI)	1
HPE Modular Storage Arrays (MSA)	3
HPE Storage Shelves	8
HPE Tape Library	2
Desktops	311
Laptops	17
Microsoft Surface Pro	374
Microsoft Surface Laptop	130
Microsoft Surface Book	13
Microsoft Surface Go	15
Panasonic Toughpads	98
Docking Stations (Laptops & Surface Devices)	636
Docking Stations (Toughpads)	173
Monitors	1159

Non-Standard Printers (not Apogee devices)	7
Multi-Function Devices	52
Desktop Print Devices	12
Security Appliance – Tier 1 (≤£2000)	6
Security Appliance – Tier 2 (≥£2000)	8
Router – Tier 1 (≤£2000)	24
Router – Tier 2 (≥£2000)	2
Switch – Tier 1 (≤£2000)	65
Switch – Tier 2 (≥£2000)	14
Wireless Controller	2
Wireless Access Points	140
Mitel IP Sets	683
SIKLU Radio Link	8

Miscellaneous	Quantity
Smartphones (Samsung)	329
iPhones	24
Non-Smartphones (Alcatel/Nokia)	364
iPads	4
Encrypted USB devices	141
Projectors (includes Smartboards)	21
Barco Click Share	53
Professional Displays	21
Clevertouch Screen	32
IPTV - Gateways	1
IPTV - Receivers	42
Remote Access Tokens	169
Running Call Phones	23

Return to Top.

Appendix B – Key D&T Projects and Activities



[Return to Top.](#)

Appendix C – 2026/27 to 2030/31 ICT Five Year Capital Plan

ICT Capital Programme 2026/27 to 2030/31

Type of Capital Expenditure	Total Cost £	2026/27 £	2027/28 £	2028/29 £	2029/30 £	2030/31 £
IT002 ICT Software						
Software Licences	**10,000**	2,000	2,000	2,000	2,000	2,000
MDT Software Solution Refresh	**175,000**	100,000				75,000
Security Info & Event Management Software	**494,000**	100,000	98,500	98,500	98,500	98,500
3 Yr Firewall	**10,000**			10,000		
3 Year PRTG Subscription License	**15,000**			15,000		
3 Year Mitel Software Upgrade	**20,000**		10,000			10,000
Threat Defence License	**57,000**	17,000	10,000	10,000	10,000	10,000
Microsoft EA Agreement (Enterprise Products)	**1,277,000**	251,000	256,500	256,500	256,500	256,500
Microsoft EA Agreement (E5 Security)	**423,000**	85,000	84,500	84,500	84,500	84,500
Microsoft EA Agreement (Subscription Products)	**32,500**	6,500	6,500	6,500	6,500	6,500
Microsoft EA Agreement (Additional Products)	**62,500**	12,500	12,500	12,500	12,500	12,500
	2,576,000	**574,000**	**480,500**	**495,500**	**470,500**	**555,500**
IT003 ICT Hardware						
Desktops (target 20%)	**240,000**	48,000	48,000	48,000	48,000	48,000
Laptops/Surface Pros/Tablets/Docking Stns (target 20%)	**602,500**	120,500	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%)	**62,000**	12,400	12,400	12,400	12,400	12,400
Windows 11 Hardware Upgrade	**100,000**				100,000	
Fire Control & OSR AV Refresh	**60,500**				60,500	
SHQ Conf AV Refresh	**215,000**				215,000	
TDA Conf AV Refresh	**250,000**				250,000	
Station AV Refresh	**150,000**				150,000	
SHQ Offices & TDA AV 5-year refresh	**100,000**					100,000
Backup Tape Drive 5-year asset refresh	**25,000**		25,000			
IPTV 5-year asset refresh	**36,800**		36,800			
	1,926,800	**197,900**	**259,700**	**197,900**	**973,400**	**297,900**
IT005 ICT Servers						
Server/storage replacement (target 20%)	**325,000**	65,000	65,000	65,000	65,000	65,000
Server/storage growth	**70,000**	14,000	14,000	14,000	14,000	14,000
Mitel Server Upgrade Corporate Telephony	**150,000**	150,000				
Virtulisation 5 Year Refresh	**450,000**				450,000	
SAN 5 Year Refresh	**195,000**	195,000				
	1,190,000	**424,000**	**79,000**	**79,000**	**529,000**	**79,000**
IT018 ICT Network						
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)	**140,000**			140,000		
MDT Wireless Network Replacement	**50,000**	50,000				
Public Wi-Fi Replacement	**15,000**					15,000
5 Year Core Network Switch/Router upgrade	**600,000**				600,000	
5 Year Secondary Fire Control backup Tel/Inf refresh	**30,000**				30,000	
5 Year Wireless Access Points and Wireless Controllers	**150,000**				150,000	
5 Year PSTN replacement asset refresh	**275,000**	125,000			150,000	
	1,345,000	**192,000**	**17,000**	**157,000**	**947,000**	**32,000**

Appendix C – 2026/27 to 2030/31 ICT Five Year Capital Plan – Continued

ICT Capital Programme 2026/27 to 2030/31

Type of Capital Expenditure	Total Cost £	2026/27 £	2027/28 £	2028/29 £	2029/30 £	2030/31 £
IT026 ICT Operational Equipment						
Station Equipment Replacement	**50,000**	10,000	10,000	10,000	10,000	10,000
Crosby Refurbishment	**10,000**	10,000				
Kirkby Refurbishment	**35,000**	35,000				
MF1 Refurbishment	**10,000**		10,000			
Toxteth Refurbishment	**10,000**		10,000			
Wallasey Refurbishment	**35,000**		35,000			
SHQ Refurbishment	**30,000**				30,000	
5 Yearly Station UPS Replacement	**70,000**					70,000
LRAD/VLS Replacement	**70,000**					70,000
GPS Repeater 5-year asset refresh	**55,000**		55,000			
Toughpad Asset Refresh - Vehicles	**150,000**	150,000				
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				
	895,000	**575,000**	**120,000**	**10,000**	**40,000**	**150,000**
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	**60,000**	30,000			30,000	
Replacement of PfSense Firewalls	**100,000**					100,000
	170,000	**32,000**	**2,000**	**2,000**	**32,000**	**102,000**
IT058 New Emergency Services Network (ESN)						
ESN Radios / Infrastructure	**54,300**	54,300				
	54,300	**54,300**				
IT063 Planning Intelligence and Performance System						
PIPS System upgrade	**120,000**				120,000	
	120,000				**120,000**	
Other IT Schemes						
IT030 ICT Projects/Upgrades	**25,000**	5,000	5,000	5,000	5,000	5,000
IT033 Incident Ground Management Software	**50,000**	50,000				
IT055 Fire Control ICT (Non Vision)	**25,000**	5,000	5,000	5,000	5,000	5,000
IT059 ESMCP Project Control Room Integration	**66,100**	66,100				
IT062 Capita Vision 5 Update - ICCS ITHC	**50,000**	10,000	10,000	10,000	10,000	10,000
IT066 ESN Ready	**20,700**	20,700				
IT067 DCS Upgrade	**226,000**				226,000	
IT068 TDA Command & Control Suite	**350,000**				350,000	
IT070 H&S Application Renewal/Replacement	**50,000**	50,000				
IT073 CAD Replacement	**2,000,000**			2,000,000		
	2,862,800	**206,800**	**20,000**	**2,020,000**	**596,000**	**20,000**
	11,139,900	**2,256,000**	**978,200**	**2,961,400**	**3,707,900**	**1,236,400**

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 Function	Status
Database used by IIT to record and report on data relating to incident investigations.	Mainstream
Financial reporting tool	Mainstream
Finance, stores and procurement package.	Mainstream
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
Committee decisions management system used to manage authority business including ensuring relevant papers are published to members via the MFRA web page.	Mainstream
HR and payroll functionality to manage the entire employee lifecycle from recruitment to staff development, succession planning and payroll.	Mainstream
Software used by People and Organisational Development to produce organisational charts using the data exported from the HR system.	Mainstream
Scanning and document management solution used in People and Organisational Development.	Mainstream
Vehicle Fleet Management System.	Mainstream

Equipment/asset management system. Used on stations to ensure operational equipment is checked regularly and appropriately maintained.	Mainstream
BA (Breathing Apparatus) testing software.	Mainstream
Virtual reality incident command training software for emergency services.	Mainstream
CAD (Computer Aided Design) software used to create and amend building plans.	Mainstream
Training Resource Planner used at the Training and Development Academy.	Mainstream
Black box data logger on vehicles.	Mainstream
CAD (Computer Aided Dispatch) This system logs all incoming emergency calls and supports the mobilisation of appropriate resources for incident management.	Mainstream
ICCS (Integrated Communications & Control System) integrated into the CAD System. This system enables Fire Control to utilise radio and telephony functions to manage incoming 999 calls and communicate with MFRS resources.	Mainstream
Management Information System providing senior officers with real time incident information and the organisation with incident history for trend analysis.	Mainstream
Data Mobilisation: Fire Control mobilise crews to incidents by sending a message to the Mobile Data Terminal (MDT) installed in the Appliance. Crews also access risk information from the MDT.	Mainstream
Internally developed SQL based application to allow the detailed recording, monitoring and assessment of fire fighter competencies against national standards for firefighters.	Prohibited
A national software application used to enhance multi-agency working.	Mainstream
Health & Safety management information system.	Mainstream
Fire specific simulation and modelling software used by Strategy and Performance for operational response planning.	Mainstream
Shift pattern modelling software used by People and Organisational Development and Operational Response.	Mainstream
TRM (Time and Resource Management) staffing system.	Mainstream
Corporate gazetteer in use across the Authority to provide standardised address information and UPRN data to corporate systems and users.	Mainstream

Reporting tool used in Strategy and Performance to extract incident data for analysis.	Mainstream
Fire and Rescue Data Platform (FaRDaP) used to record and report incident data to MHCLG.	Mainstream
System that streamlines and enhances functionality relating to station plans, business intelligence, performance management and incident mapping.	Mainstream
SharePoint Portal is used to provide the corporate intranet and central repository for MFRA core data.	Mainstream
Geographical Information System used within Strategy and Performance to display and analyse geo-spatial datasets.	Mainstream
Fuel management system.	Mainstream
Online Portal for managing the processes around e-tendering and contracts.	Mainstream
A management system used by the National Resilience Assurance Team (NRAT) and the National Coordination Centre (FRSNCC).	Mainstream
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
An application produced by our internal development team that displays real-time locations and response coverage of MFRS appliances.	Mainstream
Learning Management System.	Mainstream
Water management solution that manages data relating to hydrants.	Mainstream
Secure national web platform for exercising, planning, response, recovery, information sharing, and mapping across multiple agencies.	Mainstream
Geographical Information System (used within Strategy and Performance) to create mapping and display and analyse geo-spatial datasets.	Mainstream
Cloud based fire control specific training application for training new staff at recruit level in call handling within a controlled environment.	New
AI-enabled platform for screening application responses in recruitment campaigns.	New

Return to Top.