ICT Asset Management Plan

2018 - 2023

Table of Contents

ICT Asset Management Plan

1 Overview

1.1 Information & Communication Technology (ICT)

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 functional, flexible ICT Infrastructure possible, 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, Application Lifecycle Management and best practices, such as the Information Technology Infrastructure Library (ITIL) can lead to improvements in efficiency, performance and cost management.

ICT can be split into six key delivery areas:

- The ICT Infrastructure - Data Network, Voice & Radio Networks, Personal Computers & Devices, Servers, Printers, etc.
- Commodity Applications which run on the ICT Infrastructure - SQL, Oracle, Microsoft Office and E-Mail
- Fire Control Applications which run on the ICT Infrastructure - Vision FX CAD, Vision FX BOSS, SEED, S.t.A.R.S
- Financial Applications which run on the ICT Infrastructure - ABS E-Financials and Resource Link
- Corporate Applications that runs on the ICT Infrastructure - Tranman, PIPS, the Portal, SOFSA and Sophtlogic
- 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)

The Authority has an in-house ICT team of staff which proactively manages the existing outsourced ICT Managed Service Contract with its ICT partner telent. ICT and telent ensure the maintenance of vital '999' emergency response infrastructure, as well as continuing to expand the use of ICT technology so as to manage our resources more effectively in line with the risks facing fire-fighters, the communities of Merseyside and the organisational processes of the Authority.

ICT Infrastructure Lifecycle Management, carried out by telent on behalf of the Authority is done so in line with best practice from the ITIL framework. The processes are mature and at the same time provide an infrastructure that is robust, secure, reliable and resilient; telent continue to deliver savings and innovation through supporting initiatives such as the Multi-Function Device (MFD) contract renewal, whilst continuing to provide a high-performing ICT Service Desk.

ICT and telent are responsible for Application Lifecycle Management of Commodity and Fire Control Applications, whilst the Finance Team and the Strategy and Performance Directorate are responsible for Application Lifecycle Management for Corporate and In-House Developed Applications.

1.2 Asset Management

ICT Asset Management, carried out by ICT on behalf of the Authority, is done so in line with ITIL. ITIL is a set of best practices and processes for the management of the ICT Infrastructure and the delivery of services and support.

In line with the organisation's policy for Asset Management, the physical 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 environment impact
- An effective control structure is established for ICT Asset Management

Further information on how ICT 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 ICT Asset Management (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 environment.

Under ITAM, ICT 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:

ICT has all of its ICT Assets recorded in a Configuration Management System. This system is a database which records details of all the ICT assets and their age, thus enabling ICT to effectively manage the lifecycle of its Infrastructure. The database where the Asset information is held is on a Service Management System called "Remedy". This gives the benefit of being able to link ICT Incidents, Assets and People to enable a more in-depth trend analysis to be performed around ICT Asset Management decisions.

ICT 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.

ICT has a robust reporting process to provide systematic and timely reporting of compliance and performance, enabling prompt asset-related decision-making regarding ICT Assets

ICT has a Service Pipeline. The Service Pipeline comprises new ICT services under development and these developments lead to new or change of use of ICT Assets (See Section 5 ICT Assets Service Pipeline for further details).

To manage the ICT Five Year Capital Asset Investment Plan, ICT classifies spend into four categories:

- Underlying Spend
- ICT Project Spend
- IRMP (Integrated Risk Management Plan) Project Spend
- Fire & Rescue Service (FRS) National Project Spend

ICT has a five year lifecycle renewal policy for ICT hardware Assets such as personal computers and servers, at which point ICT Assets will be considered end of life.

ICT 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.

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

Adopting a best practice, Asset Management and Configuration Management solution allows ICT to understand:

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

As a result, the following benefits have been realised:

- Accurate information on all ICT Assets, providing ICT with the ability to deliver and support its services
- Trend analysis can be carried out against Assets to aid Incident and Problem solving
- Improved ICT security through advanced ICT Asset control
- Improved financial planning through clear identification of all assets and their associated relationships
- Improved software license management, ensuring legal compliance
- Increased confidence in ICT Systems and ICT 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 a purchase date
- Identification of current & 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, ICT has a Definitive Software Library (DSL) to improve the way it tracks software and performs Application Lifecycle Management.

Return to Top.

3 ICT Infrastructure Asset Monitoring Activities

ICT maintains an up-to-date Service Catalogue which outlines all the ICT services provided. Included in this the catalogue are references to Capacity Planning, Security and Preventative Maintenance, all of which are examples of activities carried out on ICT Assets.

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 ICT.

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)."

Security

"The Authority requires multiple levels of security on Managed Devices to defend against malicious behaviour and mitigate the risk to the Authority

The Authority utilises 3ami Monitoring and Audit System (MAS) to track changes to hardware and software throughout the organisation. MAS captures and securely stores records of all user activity including internet, email, word processing, spreadsheet applications, instant messaging and online activity.

Sophos Endpoint Protection is used to secure the Authority's systems, including, but not limited to, Windows Servers, Windows Desktops, Windows Laptops, i-pads and mobile devices against viruses, malware, advanced threats and targeted attacks.

Mobile Device Management is provided by Sophos Mobile Control and Good for Enterprise, used to secure corporate mobile devices and tablets. Features include remote lock, remote wipe, location finder, reset passwords, remote install/uninstall of applications and decommissioning.

Websense is used to protect End User devices from spam, viruses and other malicious threats via email and internet. The solution configuration is hybrid hosted and on premise.

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

Device Preventative Maintenance

"telent is responsible for device preventive 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.

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

Patching is one of the most important parts of a Cyber Security strategy keeping the ICT Infrastructure on the latest version in most cases means greater security.

Windows critical updates are installed via the WSUS server and recommended updates are reviewed and tested before installing on End User Devices.

As for the wider patching policy, the Authority is patching on assessment of risk. This policy is prudent, balancing the need to reduce the amount of down time to critical systems

Where possible Sophos Mobile control is used to manage 'non-windows' devices.

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

N.B. The full ICT Service Catalogue is too large to be an attachment but it can be accessed on request to ICT.

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. ICT prepares and publishes the following reports to fulfil this function:

Service Desk Performance Report – Monthly

The monthly ICT Service Desk Performance Report is provided to enable telent, ICT 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 ICT and IM Strategy Meetings.

ICT Infrastructure Usage Report – Monthly

The monthly ICT Infrastructure Usage Report is provided to enable telent, ICT 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.

Information Security Report – Quarterly

The monthly Information Security report provides telent, ICT 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 Meeting.

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.

Major Incident Management Reports – Ad Hoc

Whenever a Major ICT Incident takes place, a Major Incident Management Report is produced and reviewed with a view to establishing lessons learnt and to feed back into ICT Service catalogue.

Return to Top.

5 ICT Assets Service Pipeline

The Service Pipeline comprises of new ICT services under development and these developments lead to new, or change of use of, ICT Assets. ICT has six main areas associated with the Service Pipeline:

- ICT Service Requests
- ICT Business Relationship Management
- ICT Continuous Service Improvement (CSI)
- Lifecycle Management
- ICT Strategic Framework
- ICT and Information Management (IM) Steering Group
- Other ITIL Standards

A full list of Key ICT Projects can be found in Appendix B – Key ICT Projects and Activities.

5.1 ICT Service Requests

The ICT Service Desk issue ICT Request forms to allow users to request simple technical changes, information, enquiries or hardware and software changes, e.g. mobile phones.

For certain ICT requests, an approval route through the ICT Infrastructure manager is needed. The ICT request process is fully integrated in the Configuration Management System, with all changes being documented.

5.2 Business System Relationship Management

Reporting to the Head of Technology; the Business Relationship Manager (BRM) acts as the liaison between ICT and the organisation to understand its strategic and operational needs. The BRM acts as a single point of contact for senior stakeholders, ensuring understanding of available and future ICT Infrastructure Services and promoting financial and commercial awareness in order to deliver value-for-money.

Representing the organisation's needs and interests within ICT, contributing to the ICT Continual Service Improvement process (see below), assisting with the supervision and prioritisation of ICT Infrastructure Services projects.

5.3 ICT Continuous Service Improvement (CSI)

The purpose of the ICT 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 ICT department, and the key benefits have been:

- Clarity of ownership
- Clarity of requirements
- Clarity and management of cost
- 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 archive

5.4 Lifecycle Management

The ICT challenge is to provide the most functional, flexible ICT Infrastructure possible, to host the Applications that deliver benefits to the organisation, all at the lowest cost of ownership. Meeting that challenge systematically through having the right people in the right structure, Infrastructure Lifecycle Management, Application Lifecycle Management and best practices such as ITIL can lead to improvements in efficiency, performance and cost management.

ICT Infrastructure Lifecycle Management

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

ICT Application Lifecycle Management

Encompasses the planning, design, acquisition, implementation, and management of all the elements comprising Fire Control and Commodity Application Portfolios.

ITIL

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

5.5 ICT Strategic Framework

The ICT Strategic Framework is a cycle of four meetings that takes place on an annual basis and the output feeds into the ICT and IM Steering Group.

The ICT 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 ICT Strategic Framework ensures that the ICT Managed Services Contract:

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

5.6 ICT and Information Management (IM) Steering Group

The purpose of the ICT and IM Steering Group is to ensure that ICT, Application Provision and IM are co-ordinated and aligned to ensure the mission and objectives of the Authority are delivered as effectively as possible.

5.7 Other ITIL Standards

- A CAB (Change Advisory Board) 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 ICT

- ICT maintain and develop a Definitive Software Library (DSL). 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)

- ICT set minimum release management standards which third party suppliers are expected and contracted to reach

Return to Top.

6 ICT Asset Replacement Policy

ICT 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 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 ICT, the following applies:

- For small quantities of ICT Commodity items; the Authority's ICT outsourced partner will seek quotes and Authority will purchase

- For large quantities of ICT Commodity items; the Authority's ICT outsourced partner will specify requirements but the Authority's Procurement will run mini-competitions and Authority will purchase

- For ICT Assets which require complex installation or if priority support is required; the Authority's outsourced partner specify and purchase the item on the Authority's behalf and then the Authority pays via change control

- In such cases the Authority's ICT outsourced partner are requested to run a mini-competition and produce options for the Authority to select

- Purchase is done via the Contract Change Control procedure, and the Change Control Note (CCN) is signed off by ICT, 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

ICT has in place procedures for the disposal of ICT Assets via a company called "Computer Waste". Computer Waste is an ATF (Authorised Treatment Facility), fully registered by the Environmental Agency (EA). The company specialises in the recycling of Waste Electrical and Electronic Equipment (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 a member of telent, and an accompanying destruction certificate is presented to the Authority for audit purposes

6.3 Fire Control Applications and Infrastructure Assets

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

- Computer Aided Despatch (CAD); this is where incoming emergency calls are logged and the appropriate resources mobilised to incidents. The Authority uses the Vision 3 FX CAD application

- Management Information; providing senior officers with real time incident information, and the organisation with incident history for trend analysis. The Authority uses the Vision 3 FX BOSS application

- An Integrated Communications Control System (ICCS); An ICCS is found at the centre of modern-day control rooms and the Authority has a Capita DS3000. All communications that go into the control room such as 999 telephony calls, administration telephony calls, radio communication and CCTV, plug in to the ICCS. The control room staff then can manage these communications by accessing the ICCS from one place on their desktop

- Wide Area Radio Scheme; Emergency services rely on seamless radio communications coverage to effectively perform their daily tasks. The Authority, in line with the Police and Ambulance, uses Airwave

- Data Mobilisation; Fire Control can mobilise crews to incidents by sending a message to the Mobile Data Terminal (MDT) installed in the Appliance. The Authority uses the SEED application

- The Station-End Turnout solution installed in every Community Fire Station is comprised of a number of various hardware and software components and subsystems. 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.

Reporting to the Head of Technology, the ICT Application and Infrastructure Manager (Fire Control) 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
- 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

In previous years the production of an individual business case for any major Fire Control Projects secured necessary approval and capital funding. Such projects will now form part of the ICT Five Year Capital Plan

In 2018/2019 provision of £500k has been approved for the upgrade of the Computer Aided Despatch (CAD) Application.

As part of the forthcoming 2018/2019 Capital budgeting process £925k to refresh the Command & Control ICT Infrastructure will be included.

6.4 ICT Infrastructure Assets

ICT has a five-year lifecycle renewal policy for ICT hardware Assets such as personal computers, mobile devices and servers, at which point ICT Assets will be considered end of life. A three-year equipment life was considered but the increased capital spend was deemed to be excessive.

Further the proliferation of devices along the wide spectrum of Information and Communication Technologies (ICT) presents opportunities and challenges to ICT, as well as budget challenges to the organisation. There is a policy of using shared Multi-Function Devices (MFD) and having one MFD per Function to replace printers. This printer rationalisation has contributed to budget savings. ICT will rationalise the use of multiple devices and in such cases users should have access to a devices in line with RBR.

RBR is undertaken by ICT, evaluating the agile provision of ICT equipment at stations, SHQ, TDA, Vesty One and 'incidents', based on the roles of the staff housed or present there.

In 2018/2019 an ICT Asset Based Resourcing (ABR) initiative will be undertaken as a check and balance to RBR, ensuring Operational Vehicle Assets match the role of Fire Fighters and Senior officers who use such vehicles.

ICT 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.

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.

6.5 ICT Commodity Application Assets

ICT is responsible for ensuring the Authority has an Application Lifecycle Management strategy for all its Commodity Applications. ICT Works closely with all departments to develop and manage organisational Commodity Applications and agree and monitor ICT application SLAs.

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 and Office, the Authority has renewed its Microsoft EA April 2017 for a further 3 years.

As part of that renewal, the Authority secured a special price for the Microsoft SPE E3 bundle. The bundle is a secure and productive way to work that brings together the best of Office 365, Enterprise Mobility + Security, and Windows 10 Enterprise.

Anti-Virus and E-Mail Filtering

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

The ICT-selected E-Mail filtering Software "Websense" (also referred to as Surfcontrol) is used to filter email 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 licenses for the anti-virus and e-mail filtering products are procured on a three-year lifecycle and, prior to renewal, a fit-for-purpose exercise is carried out.

6.6 Corporate & Financial Application Software

The ICT BRM, as well as acting as the liaison between ICT and the organisation, has a key role to work with Strategy and Performance aligning their Corporate Application Lifecycle Management to the ICT Infrastructure, and with Finance to align theirs's.

Going forward from 2019 it proposed that the overall Asset Management Plan be amended to include the Asset Management Plans for the two departments mentioned.

6.7 Asset Movements 2017/2018

The key Assets Movements to highlight in 2017/2018 are:

- The renewal of the Konica Minolta contract was taken as a paper to members on 29th June 2017. 'CFO/043/17 Multi-Functional Device (MFD) Contract 2017 Renewal'. This initiative was key in achieving printer rationalisation and the number of HP printers reduced from 109 to 10 with the number of MFDs decreasing from 55 to 53 and the number of MFD Desktop printers decreasing from 39 to 13.

- The retirement of 78 Blackberry devices and the rollout of Windows Phones to Senior Officers and Advocates has seen the number of Smart phones rise from 2 to 154.

- The number of Desktops and Laptops have seen a small increase; however, this trend is expected to be reversed in 2018/2109 as RBR introduces tablets as a preferred way of working.

- At the time of writing there is an expected delivery of 58 Panasonic tough pads to replace the Panasonic Tough books which have reached end of life.

- The legacy, THORCOMM Automatic Vehicle Location Service (AVLS) was retired in 2017/2018 resulting in 90 Data SIM contracts being cancelled.

Return to Top.

7 ICT Asset Capital Spend Strategy

To manage the ICT Asset Investment process, ICT classifies spend into four categories:

- Underlying Spend
- ICT Project Spend
- Incident Risk Management Plan (IRMP) 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
Incident Risk Management Plan (IRMP) Project Spend	Spend on Specific IRMP Projects where ICT is a major enabler. e.g. Station Change	This spend delivers the Authority's IRMP	Safer, stronger communities; safe effective Fire fighters. Releasing budget for frontline resources
National FRS Projects	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 the National Resilience

The 2018/2023 Five Year Capital Plan can be found in Appendix C – 2018/2023 ICT Five Year Capital Plan

Return to Top.

Appendix A – Summary of ICT Infrastructure Assets

Fire Control Services and Infrastructure	Quantity
Physical Servers (Licensed as part of C&C Solution)	19
Virtual Servers (Licensed as part of C&C Solution)	1
C&C Desktops (Licensed as part of C&C Solution)	27
C&C Monitors	27
DS3000 ICCS Server	1
DS3000 ICCS Client	20
DS3000 ICCS touchscreen	20
Capita VAIU	20
Airwave San H radio gateway	1
Stateboard	3
Alerter Masts	12
Alerter Devices (multitone)	178
UHF Radio Set 2 (GP340)	149
UHF Radio Set 3 (GP340 Atex) for breathing apparatus	42
UHF Radio Set 4 (F61)	11
UHF Radio Set 5 (M1 Euro)	18
Station End Mobilising Processors	26
Station End Turnout Printers	36
Station End Auxiliary Relay Unit (ARU)	32
Station End Amplifiers	35
Station End UPS	40
IMT/IGMS Vehicles	2
Packets Atex/Marine Band/Motorola	266
Fire Control Headsets	40
Mobile Data terminals	99
Mobile Data Terminal touchscreen	98
Appliance printers	85
Airwave mobile radio SAN A	115
Airwave SAN J Radio	65
Airwave SAN B Radio	11
MDT Pump Bay Voice Terminal	85

Administration Infrastructure, Managed Servers & Desktop	Quantity
Physical Servers	82
Virtual Servers	98
Desktops *(A limited number of users have two monitors*)	594
Laptops *(Most People have an external monitor)*	332
Docking Stations (Most Laptop Users have an external monitor)	162
Tough Books	60
Monitors	771
HP Printers	10
Brother Printers	2
Konica Minolta Multi-Function Devices (Contracted to August 2022)	53
Konica Minolta Desktop Print Devices (Contracted to August 2022)	13
ASA 5515X - Security Appliance	5
ASA 5510 - Security Appliance	3
Router c819	2
Router c2921	2
Router c1841	23
Router c1921	7
Switch c4510r+e	1
Switch c3750G-24	1
Switch c3750G-48	1
Switch c3750-48	13
Switch c3750V2-48	7
Switch c3560G	2
Switch c3560E	3
Switch c3560X	2
Switch c3560	1
Switch c3550-48	17
Switch c3550-24	20
Switch c2960G-24	2
Switch c2960G-48	4
Switch c2960S-24	6
Switch c2960S-48	4
AIR-CT5508-K9	2
LAP1141N	9
LAP1142N	48
HP MSM325	28
HP MSM460	2
Cisco 1800 *(Telewest Managed Router at SHQ)*	1
Mitel Mxe	4
Mitel Cxi	6
Mitel IP Sets	700
Mitel 5310 Conferencing Phones	10
HP Tape Library 8096	1

HP 2312i Primary SAN	1
HP 2012i Secondary SAN	1

Miscellaneous	Quantity
Mobile Phones	483
iPhones	20
Smartphones	154
MTPAS Enabled Mobile SIMS	96
MDT Enables Data SIMS	87
iPad	54
Tablets (includes new MDT2 hardware x 37)	49
USB Encrypted USB devices	183
3G Cards/Dongles	23
Modem	51
Fax	8
Scanners	8
Battery Chargers	142
CD Writers	3
CCTV Monitors	12
CCTV VCR	12
Smart Boards	31
Conference Audio Visual	1
IPTV - Server	1
IPTV - Gateways	3
IPTV - Receivers	29
Remote Access Tokens (Celestix)	100
Door Access Controller Server	1
Door Access Controllers	15
Door Access Card Printer	1
Door Access Cards	313
Door Access Proximity + Pin Readers	15
Door Access Push to Exit buttons	13
Door Access Break Glass Units	13
Running Call Phones	31

Appendix B – Key ICT Projects and Activities

ITHC Remedial Work Plan v7
Jan-18

On-Hold
Work in progress
Planned Completion/Go Live
Work Complete

		2017			2018												2019	Update
		Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June	July	Aug	Sep	Oct	Nov	Dec		
HC01	Replacement of Station Turnout Equipment (HC01)					2 Station POC					Rollout Complete							Procurement ongoing
HC02	Additional use of IT tools and applications to better define the security status of the network (Nexthink)					order raised	Complete											Procurement ongoing
HC03	In line with ESN requirements to record a greater detail of system events and logs. (LogPoint)		Order raised				Rollout Complete											LogPoint Ordered. Scheduled in with suppliers for Feb 18
HC04	Implementation of a clearly defined Patching regime in line with ESN requirements that covers MS, Non MS and Manufacturer patches through use of tools e.g. SCCM				Complete			Complete										Server Patching Phase 1 compled Jan 2018. Next Phase scheduled for April 18. Client patching to be scheduled for Mar 18
HC05	Vision Clients upgrade to Windows 10						Installed											Delayed due to MDT issues in October and November and Prescot effort
HC06	Retire unsupported Clients							Complete										Ongoing
HC07	Removal of unsupported Windows Server OS and DB version									Complete								Ongoing
HC08	Removal of unsupported Linux Server OS							Complete										Ongoing
HC09	Upgrade of legacy telephony solution														Complete			Procurement to begin 2018
HC10	Upgrade to Public Wi Fi					Complete												on track
HC11	Apply tighter policies or GPO on individual clients / servers to resolve information disclosure / host breach / security misconfiguration (3 month plan)					Complete												Ongoing
HC12	ESN Code of Connection (FC002)						Approved											Ongoing
HC13	CNS to undertake repeat ITHC									Repeat ITHC								on track

Fire Control Roadmap 2018 Version 6
Jan-18

On-Hold
Work in progress
Planned Completion/Go Live
Work Complete

			2017			2018												2019	Update
			Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June	July	August	September	October	November	December		
ITHC	FC001	General Remediation Works									Repeat ITHC								Detailed in the ITHC Roadmap
	FC002	ESN Code of Connection (HC12)						Approved											
	FC003	Replacement of Station Turnout Equipment (HC01)					2 Station POC					Rollout Complete							
Capita	FC004	ICCS Wanna Cry Patching	Complete																Complete
	FC005	Control Room Integration to ESN												Complete					Order Placed. Project launched in December 2017. MFRS allocated slot end of March 2018. Phase 2 dependant on ESN device availability.
		- DNSP (Direct Network Service Provider) Link						Installed											
		- ICCS ESN p1 2017 R1 ESN Baseline						Installed											
		- ICCS ESN p2a Deploy NATS approved software										Installed							
		- ICCS ESN p2b ESN integration tests												Complete					
	FC006	Vision Clients upgrade to W10 (HC05)						Installed											Delayed due to MDT issues in October and November and Prescot effort
	FC007	Vision Server 2 HW refresh for Resilience(others may follow)						Complete											
	FC008	Vision Network Refresh									Complete								
	FC009	CAD & MIS Upgrade					1st Project Board											Go-Live	Date TBA
MDT	FC010	MDT Upgrade project (Full risk info or 15 minutes?)					Order Placed				Complete								Significant work has continued to understand the requirements for Risk information. Work around potential change to MDT HW. Order placed in Feb
Fire Control CSI	FC011	*Upgrade to SAN H (Go live - how close to ESN?)*	On Hold																On Hold
	FC012	Upgrade to ISDN 18																	On Hold
	FC013	SEED MDT Maps upgrade																	To be scheduled
	FC014	WTR Mobilisation																	On Hold
	FC015	Increased Buddy Arrangements																	On Hold
Other	FC017	STARS hosting	On Hold																On Hold
	FC018	A365 hosting	On Hold																On Hold
	FC019	Ops planning integration	Complete																Complete
	FC020	Prescot Fire Station				Complete													Complete

Appendix C 2018/2023 ICT Five Year Capital Plan - Draft

ICT - Approved Budget 2017/18 to 2021/22

Type of Capital Expenditure		Total Cost £	2017/18 £	2018/19 £	2019/20 £	2020/21 £	2021/22 £	2022/23 £
IT002 ICT Software								
Software Licences		25,400	15,400	2,000	2,000	2,000	2,000	2,000
New Virtualistation Infrastructure		75,000		75,000				
3 Year Licences Antivirus & Filtering		169,000	169,000					
5 Year Antivirus & Filtering Software		200,000						200,000
MDT Software Solution Refresh		100,000						100,000
Microsoft EA Agreement (Servers & Security)		297,000	57,000	48,000	48,000	48,000	48,000	48,000
Microsoft EA Agreement (Windows & Office)		768,000	128,000	128,000	128,000	128,000	128,000	128,000
Microsoft EA Agreement (Application Development)		30,000	5,000	5,000	5,000	5,000	5,000	5,000
Microsoft SQL Upgrade								
		1,664,400	**374,400**	**258,000**	**183,000**	**183,000**	**183,000**	**483,000**
IT003 ICT Hardware								
Desktops (target 20%)		246,250	45,750	40,100	40,100	40,100	40,100	40,100
Tablets & Docking Stations (target 20%)		442,000	102,000	92,000	62,000	62,000	62,000	62,000
Toughpads		110,000	110,000					
Monitors & Monitor Arms (target 20%)		85,400	15,400	14,000	14,000	14,000	14,000	14,000
Peripherals replacement (target 20%)		18,000	3,000	3,000	3,000	3,000	3,000	3,000
Mobile device replacement (target 20%)		44,100	4,100	28,000	3,000	3,000	3,000	3,000
Replacement Backup Tape Drive		25,000					25,000	
IP TV Asset Refresh		50,000			50,000			
Audio Visual Conference Facility		120,000				120,000		
		1,140,750	**280,250**	**177,100**	**172,100**	**242,100**	**147,100**	**122,100**
IT005 ICT Servers								
Server/storage replacement (target 20%)		390,000	65,000	65,000	65,000	65,000	65,000	65,000
Server/storage growth		130,000	15,000	15,000	25,000	25,000	25,000	25,000
New SAN Solution		48,400	48,400					
		568,400	**128,400**	**80,000**	**90,000**	**90,000**	**90,000**	**90,000**
IT018 ICT Network								
Local Area Network replacement (discrete)		20,000		4,000	4,000	4,000	4,000	4,000
Network Switches/Routers replacement		264,500	94,500	170,000				
Network Switches/Router growth		25,000		5,000	5,000	5,000	5,000	5,000
Network Switches/Router - Additional for JCC/TDA Resilience		10,000			10,000			
Vesty Road Network Link Refresh		40,000			40,000			
IP Telephony		150,000	150,000					
Wireless Network		40,000		40,000				
		549,500	**244,500**	**219,000**	**59,000**	**9,000**	**9,000**	**9,000**
IT026 ICT Operational Equipment								
Pagers/Alerters		35,000		7,000	7,000	7,000	7,000	7,000
Station End Kit		36,000	11,000	5,000	5,000	5,000	5,000	5,000
Incident Ground Management System		50,000		50,000				
MDT Replacement (Not incl. in ESMCP)		120,000				120,000		
		241,000	**11,000**	**62,000**	**12,000**	**132,000**	**12,000**	**12,000**
IT058 New Emergency Services Network (ESN)								
ESN Radios / Infrastructure - Estimate	#	150,000	95,000	55,000				
		150,000	**95,000**	**55,000**				
IT060 ICT Station Change								
Saughall Massie Station End Mobilising Equipment				20,000				
St Helens Station End Mobilising Equipment				20,000				
General			7,000					
		47,000	**7,000**	**40,000**				
SHQ/JCC Major Refurbishment								
IT051 JCC Airwave Solution		5,200	5,200					
IT053 JCC Backup MACC/Secondary Control Resilience		39,500		39,500				
		44,700	**5,200**	**39,500**				
Other IT Schemes								
IT019 Website Devolpment		50,000	50,000					
IT027 ICT Security - Remote Access Security FOBS		12,000	2,000	2,000	2,000	2,000	2,000	2,000
IT028 System Development (Portal)		149,700	39,700				110,000	
IT030 ICT Projects/Upgrades		29,300	4,300	5,000	5,000	5,000	5,000	5,000
IT055 C.3.I. C.& C Communication & Information System		30,000	5,000	5,000	5,000	5,000	5,000	5,000
IT056 Door Access System		8,600	8,600					
IT057 Fleet Management System		4,600	4,600					
IT059 ESMCP Project Control Room Integration		324,000	324,000					
IT061 ESMCP ITHC Remedial Works		111,300	111,300					
FIN001 FMIS/Eproc/Payroll/HR Replacement		69,800	69,800					
NEW Capita Vision 3 Update (CFO/058/17)		500,000			500,000			
		1,289,300	**619,300**	**12,000**	**512,000**	**12,000**	**122,000**	**12,000**
		5,695,050	**1,765,050**	**942,600**	**1,028,100**	**668,100**	**563,100**	**728,100**

Return to Top.