ICT Asset Management Plan

2016 - 2021

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 that challenge systematically through having the right people in the right structure, Infrastructure Lifecycle Management, Application Life Cycle Management and best practices such as ITIL (Information Technology Infrastructure Library) can lead to improvements in efficiency, performance, and cost management.

ICT can be split into five key delivery areas

- ICT Infrastructure (Data Network, Voice & Radio Networks, Personal Devices, Servers, Printers etc.)
- ICT Service Desk
- Commodity Applications that run on the ICT Infrastructure (Microsoft Office & E-Mail)
- Fire Control Applications that run on the ICT Infrastructure (Vision FX CAD, Vision FX BOSS, ICCS, Seed and StARS)
- Corporate and 'In House' Developed Applications that run on the ICT Infrastructure (E-Financials, PIPS, Portal, Fleet Management & OSHENS)

The Authority has an in-house ICT team of five staff who proactively manage the existing outsourced ICT Infrastructure Service Provision £1.8m contract with its ICT partner telent. ICT & telent ensure the maintenance of vital '999' emergency response infrastructure, as well as continuing to expand the use of ICT technology in managing our resources more effectively in line with the risks facing firefighters, the communities of Merseyside and the organisational processes of the Authority.

ICT Infrastructure Life Cycle 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 providing an infrastructure that is robust, secure, reliable and resilient; telent continue to deliver savings and innovation through initiatives such as Skype for Business, whilst continuing to provide a high performing ICT Service Desk.

ICT and telent are responsible for Application Life Cycle Management of Commodity and Fire Control Applications, whilst the Finance Team and the Strategy and Performance Directorate are responsible for Application Life Cycle 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 (Information Technology Infrastructure Library). 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 organisations policy for Asset Management, the physical life cycle 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 'life cycle' costs, benefits, and risk 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.

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 life cycle 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 ITIL ICT Asset Management, ICT manages its assets effectively to help deliver its strategic priorities and service 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 the 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 to enable prompt asset-related decision-making regarding ICT Assets

ICT has a 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 (See Section “5 ICT Assets Service Pipeline for further details).

To manage the ICT Five Year Capital Asset Investment Plan ICT classifies spend in to four categories:

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

ICT has a 5 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 role is reviewed and if still 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 provides 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 the Service Management application, 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

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.

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 the 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 their 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 Authorities 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 Authorities 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.

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

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".

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

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 prepare and publish the following reports to fulfil this function.

Service Desk Support 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, against the Service Delivery standard detail in the Authority's Service Provision Agreement Dated April 2009.

ICT Infrastructure Usage Report – Monthly

The monthly ICT Infrastructure 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 – Monthly

The monthly Information Security report provides telent, ICT and the Authority's officers (including 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 Information Security Forum.

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.

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
- Business System Relationship Management
- ICT Continuous Improvement
- Lifecycle Management
- ICT and 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 Request

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; this role acts as the liaison between ICT and the organisation to understand its strategic, and operational needs. Acting as a single point of contact for senior stakeholders ensuring understanding of available and future ICT Infrastructure Services, promoting financial and commercial awareness in order to deliver value-for-money.

Representing the organisations needs and interest 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

The purpose of the ICT Continual Service Improvement 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, maximizing 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 Continual Service Improvement Register.

This Continuous Service Improvement (CSI) process is now firmly embedded in the ICT and the Key benefits have been:

- Clarity of ownership
- Clarity of requirements
- Clarity & management of cost
- Visibility and tracking progress
- Forward Planning
- Resource Scheduling
- Identifying duplicate effort across the Authority's departments and or stations
- Ability to utilise information from archive

5.4 Life Cycle 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 Life Cycle Management and best practices such as ITIL (Information Technology Infrastructure Library) can lead to improvements in efficiency, performance, and cost management.

ICT Infrastructure Life Cycle Management

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

ICT Application Life Cycle Management

Encompasses the planning, design, acquisition, implementation, and management of all the elements comprising an Organisation's Application Portfolio.

ITIL (Information Technology Infrastructure Library)

Is the most widely accepted approach to ICT service management in the world.

5.5 ICT and IM Steering Group

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

5.6 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 will ensure 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 for example number of users, location of users, contact details of suppliers and Service Level Agreements (SLAs).

- ICT set minimum release management standards which 3rd party suppliers are expected and contracted to reach.

6 ICT Asset Replacement Policy

ICT has in place procedures to trace the acquisition, deployment, management and disposal of ICT Assets under their 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 out sourced partner will seek quotes and Authority will purchase

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

- ICT Assets which require complex installation or if priority support is required; the Authority's out sourced partner specify and purchase the item on Authority's behalf & then Authority's pay via change control.

  In such cases the Authority's ICT out sourced partner are requested to run a mini competition and produce options for Authority's 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 Authority's ICT out sourced 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. The company specialises in the recycling of WEEE (Waste Electrical and Electronic Equipment).

- All ICT assets disposed of with Computer Waste are recorded on a waste transfer note that is signed and presented to MF&RS for audit purposes.
- Hard Drives are destroyed on MF&RS premises witnessed by a member of the ICT outsource service provider "telent", and an accompanying destruction certificate is presented to MF&RS for audit purposes.

6.3 Fire Control Applications and Infrastructure Assets

There are 5 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 the incidents. The Authority use the Vision 3 FX CAD 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 use Airwave.

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

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

Reporting to the Head of Technology the ICT Application & 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 Service Level Agreements. (SLAs). Activities include;

- Following of best practice ICT Asset Management
- The production of an individual business case for any major Fire Control Application or Infrastructure replacement or refresh.
- Spare holding to help meet SLA's.
- 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.

6.4 ICT Infrastructure Assets

ICT has a 5 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. A 3 year equipment life was considered but the increased capital spend was deemed to be excessive at this point in time.

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 5 year equipment life.

6.5 ICT Commodity Application Assets

ICT is responsible for ensuring he Authority has an Application Life Cycle Management strategy for all its Commodity Applications. Working closely with all departments to develop and manage organisational Commodity Applications and agreeing and monitoring ICT application Service Level Agreements.

Microsoft Software: Enterprise Agreement:

In 2015 Microsoft informed Licensing Solution Providers (LSPs) that PSA12 would expired on April 30th.

PSA12 was a Memorandum of Understanding (MOU) with the Government Procurement Service (GPS), and was an amended continuation of PSA09 contractual concessions and discounts which was in effect until June 30th 2012 for the Government and Public Sector

As Microsoft continues to adopt pricing and licensing models to incentivise adoption of cloud based subscription services, Microsoft have agreed a ‘cloud-first’ offer with the Crown Commercial Service (CCS) on behalf of Public Sector organisations in the UK.

The cloud first offer is called the Microsoft Cloud Transformation Agreement (CTA). The Microsoft CTA was effective from May 1st 2015, and is a non-binding Memorandum of Understanding (MoU) with the Crown.

What this means to MF&RS is that our existing Microsoft Enterprise Agreement (EA) will be in place for 2016/2017 and in 2017/2018 MF&RS will be required to move to the new Microsoft CTA.

Anti-Virus and E-Mail Filtering*:*

ICT chosen anti-virus software “Sophos” protects the Authority from computer viruses and any other threats which may try to enter Authority’s Network.

ICT chosen E-Mail filtering Software “Websense” (also referred to as Surfcontrol) is used to filter email and quarantine non legitimate e-mail 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 are procured on a 3 year life cycle and prior to renewal a fit for purpose exercise is carried out.

6.6 Corporate Application Software:

The ICT Business Relationship Manager 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.

7 ICT Asset Capital Spend Strategy

To manage the ICT Asset Investment process ICT classifies spend in to four categories:

- Underlying Spend
- ICT Project Spend
- IRMP Project Spend
- National FRS Project Spend

These are explained in the following table:

ICT Capital Spend Matrix

	Spend	Why	Benefit
Underlying Spend	Spend on the existing ICT Infrastructure including Software, Desktops, 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. Telephony	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. Alerter	This spend delivers the Authority's IRMP	safer, stronger communities; safe effective Fire fighters
National FRS Projects	Spend on Specific National projects where ICT is a major enabler.	Spend to align the Authority's systems to National Initiatives	Protecting public safety and increasing the nation's resilience

The 2016/2021 Five Capital plan can be found in Appendix C – 2016/2021 ICT Five year Capital Plan.

Appendix A – Summary of ICT Infrastructure Assets

Fire Control Services 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)	24
Monitors	24
DS3000 ICCS Server	1
DS3000 ICCS Client	20
DS3000 ICCS touchscreen	20
Sennheiser UI760 amplifier	19
Capita VAIU	19
Airwave San H radio gateway	1
Stateboard	3
Cisco 2960g	5
Cisco ASA 5510 Firewall	2
Alerter Masts	13
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	29
Station End Turnout Printers	36
Station End Auxiliary Relay Unit (ARU)	32
Station End Amplifiers	35
Station End UPS	40
IMT/IGMS Vehicles	1
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
Domain Accounts *(includes service and 3rd party accounts)*	1855
Domain Accounts *(with Internet Access)*	1420
Domain Security Groups	379
Exchange Mailboxes	1634

Exchange Distribution Lists	309
Exchange External Contacts	143
Exchange Public Folders	223
Physical Servers	85
Virtual Servers	79
Desktops *(A limited number of users have two monitors*)	602
Laptops *(Most People have an external monitor)*	278
Docking Stations (Most Laptop Users have an external monitor)	115
Tough Books	60
Monitors	800
HP Printers	109
Brother Printers	2
Konica Minolta Multi-Function Devices (Contracted to July 2017)	60
ASA 5515X	5
ASA 5510	3
Router c819	1
Router c2921	2
Router c1841	23
Router c1921	6
Switch c4510r+e (not including supervisors and linecards)	1
Switch c3750G-24	2
Switch c3750G-48	2
Switch c3750-24	2
Switch c3750-48	12
Switch c3750V2-48	7
Switch c3560G	1
Switch c3560E	3
Switch c3560X	1
Switch c3560	1
Switch c3550-48	18
Switch c3550-24	21
Switch c2960G-24	2
Switch c2960G-48	4
Switch c2960S-24	9
Switch c2960S-48	6
AIR-CT5508-K9	1
LAP1141N	9
LAP1142N	47
SAP1602I	6
HP MSM325	30
HP MSM460	2
HP 2824	7
Cisco 1800 *(Telewest Managed Router at SHQ)*	1

Mitel Mxe	4
MItel Cxi	8
Mitel IP Sets	700
Mitel 5310 Conferencing Phones	10

Miscellaneous	Quantity
Mobile Phones	470
iPhones	15
Smartphones	2
Blackberry	78
MTPAS Enabled Mobile SIMS	106
AVLS Enabled data sims	90
MDT Enables data sims	90
iPad	40
Tablets	8
USB Encrypted USB devices	150
3G Cards/Dongles	52
Modem	56
Fax	9
Scanners	9
Battery Chargers	96
CD Writers	3
CCTV Monitors	12
CCTV VCR	12
Smart Boards	32
Sony Video Conference Unit	1
IPTV - Server	1
IPTV - Gateways	3
IPTV - Receivers	40
Remote Access Tokens	100
Door Access Controller Server	1
Door Access Controllers	15
Door Access Card Printer	1
Door Access Cards	284
Door Access Proximity + Pin Readers	20
Door Access Push to Exit buttons	13
Door Access Break Glass Units	13
Smartboard and AV equipment	32
Running Call Phones	31
Panaboard	1

Appendix B – Key ICT Projects and Activities

ICT Asset Management Plan							
			Project Duration				
Appendix C - Key Projects and Activities							
		2015/2016	***2016/2017***	***2017/2018***	***2018/2019***	***2019/2020***	***2020/2021***
ICT Support for other Directorate Initiatives	Underlying ICT Support for other Directorate Natives. E.g. Station Mergers, Closures and building refurbishment including Access Control						
Emergency Services Mobile Communication Plan (ESMCP)	The Service is scheduled to switch from the current Airwave communication system to an Emergency Services Network which will provide broadband connectivity which will allow us to utilise applications additional to Radio Comms						
Future Mobile Data Terminal Solution	As a minimum the replacement of the MDT Screen & CPU. This item is not included on the ESCMCP						
Data Mobilisation Enhancement	Data mobilsation over Airwave and possible replacement of the SEED application						
Computer Aided Despatch Upgrade	Upgrade of the CAD to Vision DS Planning Workshop.						

Total Replacement of Command and Control (including new ICCS)	Subject to future collaboration initiatives it is envisaged that a new Command & Control Solution replacement program will start in 2018/2019						
New ICT Managed Service Provision	Implement Efficiency and Innovation Initiatives as proposed in recent outsource contract negotiations						
TDA Communications Room Upgrade	Replacement of the Core data Network at the TDA						
Initial Embrace of Cloud Technology	Promote collaborative working between ICT and the organisation at a project level especially in the area of 'DevOps'. Move to Microsoft Azure and fundamentally review Microsoft Licencing						
Sophos and Websense.	Five year anniversary review of antivirus and filtering software which will result in a significant upgrade or replacement activity						
Enhanced Virtualisation Infrastructure	As virtualisation becomes more of a specialist application, it is believed that to utilise this new and specialist technology, MF&RS would need to purchase and implement a new commercial off the shelf offering.						
Future Tablet Solution	Currently a mix of iPad, laptops and tough books is in place. Once the Application Development strategy is confirmed for electronic forms a tablet solution will be sought.						

IPTV Asset Refresh	Lifecycle Management replacement of the 'hotel style' TV solution in SHQ						
Audio/Visual Conference Refresh	Lifecycle Management replacement of the Audio/Visual Conference equipment & hearing loop in SHQ						
Storage Area Network(SAN)	New SAN and backup SAN for Departmental and Home Folders						
Network Refresh	Individual Network refresh of SHQ, Vesty Rd, Stations and TDA						
IP Telephony Refresh	Upgrade of the desktop telephony system						
New ICT Infrastructure for the Portal	The basic ICT Infrastructure is in place. In the future this may be modified as the Portal team upgrade to SharePoint 2013						
Hearing Loop and Wi-Fi Expansion	Adaptions to Community Fire Stations to meet current Equality Act & to provide enhanced Community access.						
Further Skype Rollout	Skype for Business is being used in ICT and by the Station Managers. Phase two would be the trial of its use for external meetings, after which it will be rolled out to all.						

Two Factor Authentication	In line with Audit recommendation and as a requirement for future Code of Connections, rollout of Celestix DAX two factor authentication. To access the network remotely staff will use a fob which generates a second password.						
		2015/2016	***2016/2017***	***2017/2018***	***2018/2019***	***2019/2020***	***2020/2021***

Appendix C – 2016/2021 ICT Five Year Capital Plan

Type of Capital Expenditure		Total Cost	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21
		£	£	£	£	£	£	£
New Emergency Services Network (ESN)								
ESN Radios / Infrastructure - Estimate		**250,000**			250,000			
IT002	**ICT Software**							
Software Licences		**12,000**	2,000	2,000	2,000	2,000	2,000	2,000
New Visualisation Infrastructure		**75,000**				75,000		
3 Year Licences Antivirus & Filtering		**169,000**			169,000			
Microsoft EA Agreement (Servers & Security)		**300,000**	60,000	60,000	60,000	60,000	60,000	
Microsoft EA Agreement (Office Desktop)		**525,000**	65,000	80,000	80,000	80,000	80,000	140,000
Microsoft SQL Upgrade		**50,000**	50,000					
		1,131,000	**177,000**	**142,000**	**311,000**	**217,000**	**142,000**	**142,000**
IT003	**ICT Hardware**							
PC, monitor and laptop replacement (target 20%)		**452,900**	72,900	80,000	80,000	80,000	70,000	70,000
PC, monitor and laptop growth		**30,000**	5,000	5,000	5,000	5,000	5,000	5,000
Peripherals replacement (target 20%)		**63,900**	33,900	6,000	6,000	6,000	6,000	6,000
Tablets (IPad)		**90,000**				30,000	30,000	30,000
LFS Laptops		**40,000**		40,000				
IP TV Asset Refresh		**50,000**					50,000	
Appliance Toughbook Replacement		**110,000**	110,000					
Audio Visual Conference Facility		**120,000**						120,000
		956,800	**221,800**	**131,000**	**91,000**	**121,000**	**161,000**	**231,000**
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		**110,000**	15,000	15,000	15,000	15,000	25,000	25,000
New SAN Solution		**100,000**		100,000				
		600,000	**80,000**	**180,000**	**80,000**	**80,000**	**90,000**	**90,000**
IT018	**ICT Network**							
Local Area Network replacement (discrete)		**24,000**	4,000	4,000	4,000	4,000	4,000	4,000
Network Switches/Routers replacement		**351,000**	81,000	60,000	100,000	110,000		

Network Switches/Router growth		**30,000**	5,000	5,000	5,000	5,000	5,000	5,000
Network Switches/Router- for JCC/TDA Resilience		**10,000**					10,000	
Vesty Road Network Link Refresh		**40,000**					40,000	
IP Telephony		**150,000**	50,000	100,000				
Wireless Network		**40,000**		40,000				
		645,000	**140,000**	**209,000**	**109,000**	**119,000**	**59,000**	**9,000**
IT026	**ICT Operational Equipment**							
Pagers/Alerters		**35,000**		7,000	7,000	7,000	7,000	7,000
Station End Kit		**25,000**		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
		230,000		**62,000**	**12,000**	**12,000**	**12,000**	**132,000**
SHQ/JCC Major Refurbishment								
IT051	JCC Airwave Solution	**99,000**	99,000					
IT053	JCC Backup MACC/Secondary Control	**57,000**	57,000					
		156,000	**156,000**					
Other IT Schemes								
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)	**226,000**	**108,000**	18,000	25,000	25,000	25,000	25,000
IT030	ICT Projects/Upgrades	**25,000**		5,000	5,000	5,000	5,000	5,000
IT034	E-Mail retention (legal requirement)							
IT037	Emerging Technologies							
IT040	Integrated Planning & Performance M.S.	**14,000**		14,000				
IT046	TRM System	**32,500**	32,500					
IT049	Wireless Rollout	**18,300**	18,300					
IT050	Community Protection IMS System	**30,000**	30,000					
IT055	C.3.I.C.&.C Communication & Info System	**83,000**	8,000	15,000	15,000	15,000	15,000	15,000
IT056	P.F.I. Door Access System	**18,000**	18,000					
IT057	Fleet Management System	**12,000**	12,000					
FIN001	FMIS/Eproc/Payroll/HR Replacement	**108,500**	108,500					
		579,300	337,300	**54,000**	**47,000**	**47,000**	**47,000**	**47,000**
		4,548,100	**1,112,100**	**778,000**	**900,000**	**596,000**	**511,000**	**651,000**