Lancashire Fire and Rescue Service ICT Plan 2022-2027

Introduction

The ICT landscape has changed considerably which has been driven by the adoption of cloud-based services, an increase in remote working as well as a significant increase in cyber threats. Data and Digital information are essential for Lancashire Fire and Rescue Service (LFRS); they are vital for improving fire response, prevention and protection services to the public. A huge amount of what LFRS does depends on the effective use of data and information.

The 2022-2027 ICT plan maximises the effectiveness and efficiency of our workforce to ensure the best possible service and levels of engagement for our communities and it ensures a strong foundation is in place that supports and underpins the delivery and development of the service's Data and Digital Strategy.

In addition, we will consider best practice guidelines from central Government together with other partner agency collaborations wherever possible. We will also look to align ourselves with established and accepted best practices and working patterns from across the technology sector.

Glossary

What is the cloud?

The cloud allows users to access the same files and applications from almost any device, because the computing and storage is on servers in global data centre accessed through the internet, instead of locally on the users' own device or network.

Why is it called the cloud?

In the early days of the Internet, technical diagrams often represented the servers and networking infrastructure that make up the Internet as a cloud and the phrase stuck.

On Premises (on prem)

On-premises software and technology, also called on-prem, is housed within the physical location of an enterprise, rather than in the cloud or on hosted servers in a remote facility.

National Cyber Security Centre (NCSC)

The LFRS Cyber Security strategy is underpinned by adopting the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF), which is the assurance framework for local Government.

Service key principles

Our culture plays an integral part in enabling the service to achieve our priorities of:

- Preventing fires and other emergencies from happening
- Protecting people and property when they happen
- Responding to fires and other emergencies quickly and competently
- Valuing our people
- Delivering value for money

Our service "STRIVE" values underpin everything we seek to achieve, which fundamentally aligns to the fire and rescue service national code of ethics:

- Service
- Trust
- Respect
- Integrity
- Value
- Empowerment

Through the key objectives set within the digital strategy, we aim to support the creation of a positive, inclusive culture that encourages innovation and continuous improvement. Achieving the right culture will enable us to deliver the best services and be an outstanding fire and rescue service for our communities and visitors.

To help achieve this, we will align our digital landscape with these organisational values to ensure that:

- Our workforce can make effective use of technology to communicate, safely store and share information
- Our workforce can work effectively from anywhere using the most appropriate device for their role, intrinsically increasing our efficiency
- Our workforce has easy access to data and intelligence relevant to their role and that the information is current to help increase safety and reduce risk
- Our workforce is digitally engaged in the organisation and champion a digital first culture
- We strive to reduce paper, printing and increase our process efficiency through digitisation and automation
- Our digital solutions focus on the needs of our communities and that they are able to engage with us in a more digitally enabled and accessible way

Service Support

The Helpdesk (Service Desk) is the front facing operating arm of the ICT department that's there to keep operations running smoothly as well as taking ICT service requests. The Helpdesk handles everything from individual technical problems to larger scales systems issues and outages and it provides a single point of contact for staff and external agencies to interact with ICT.

The ICT Helpdesk will work to re design it's processes to better align with Information Technology Infrastructure Library (ITIL) best practice guidelines and look for opportunities to extend its support services into other areas of the support departments.

What is ITIL?

ITIL, is a well-known set of IT best practices designed to assist businesses in aligning their IT services with customer and business needs. Services include IT-related assets, accessibility, and resources that deliver value and benefits to customers.

The Service Design stage focuses on developing new IT services, as well as modifying or improving existing IT services to enhance their value to the business.

We will:

- Implement a service desk portal which will allow staff members to log and monitor their own support tickets against agreed SLAs and against a catalogue of supported ICT technologies. This will be developed to include other areas of the service that provide internal application support.
- Provide automation where possible for maximum efficiency and less reliance on manual intervention. This will extend to being able to reset passwords without the involvement of ICT.
- Focus on reducing the amount of time it takes to resolve a support ticket by using service desk pods consisting of 1st, 2nd and 3rd line support staff. This model will help to ensure a ticket is closed in one round of escalation and it will also encourage cross skilling.
- Re design the asset management solution and offer that function out to other areas of the service for maximum cost savings.

Prince’s Trust

What is Prince’s Trust?

The Prince's Trust and the Fire and Rescue Service have a long and proud history of working in partnership. Since 1992, together we’ve helped many thousands of young people to change their lives through Prince’s Trust programmes.

The Trust and the FRS share many common objectives which impact on communities we serve. Our work together is guided by the values of social responsibility and inclusiveness.

ICT deliver WiFi, printing, iPads, projectors, and computers/monitors for all Prince’s Trust students.

We will:

- In 2023 replace all desk-based computers within the Prince’s Trust sites with modern Windows 10 / 11 flavours.
- Evaluate a cloud first option which is likely to be either Citrix in the Cloud or Azure Desktop.
- Provide support where needed to ensure staff have the equipment they need to deliver the support and training for the students.
- Continue to evaluate the solutions we offer to ensure they are fit for purpose in a fast-paced technology environment.

Network

Many of the service's core business functions would not operate without network connectivity, so a robust and reliable network infrastructure is essential for effective and efficient service delivery.

LFRS has several network links which connects the services 39 stations to the central data centres located at Headquarters, North West Fire Control and Service Training Centre, to Lancashire County Council for collaboration and delivery of the service's financial systems and to the Internet.

We will:

- Work with Northwest Shared Infrastructure Services (NWSIS) on the re-procurement of the current WAN contract which expires in October 2023. Engagement with the NWSIS team will commence in 2022 and involve specification and design workshops that will allow us to tailor the next iteration of the WAN to complement and underpin the strategic direction of the FRSs objectives of adopting cloud-based services.
- In 2022 invest in dedicated fast and reliable connections direct into the Microsoft Azure network, to ensure that future needs of those services remain available. These services extend to other parts of the service and are fundamental in the delivery of the services Data and Digital strategy.

What is Azure ExpressRoute?

ExpressRoute enables LFRS to extend our on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute, the Service can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.

ExpressRoute connections don't go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet.

The benefit of having a dedicated route is mainly down to speed. If we pushed all our cloud/365 traffic down our normal Internet link then we would start to see performance issues for both Internet traffic, i.e., web browsing and the cloud traffic, therefore it's best practice to separate this out.

WiFi

The current WiFi estate was installed to support a small number of features and functions and over the last five years LFRS has seen an increase in demand and reliance of WiFi.

We will:

- In 2023 procure and implement the next generation WiFi to support the service's requirement for a modern, secure WiFi implementation that allows and encourages innovation.
- Digitilise our fire appliances to provide a more efficient and effective service to our communities, maximising the productive time of our firefighters and officers when they are off station. The digitisation of the appliances, including the replacement of our current Mobile Data Terminals will be a key focus for the service during 2023-24.
- Following the global Coronavirus pandemic, we will continue our digitisation improvement journey including improving the use of Microsoft Teams and other digital platforms across the service.
- Our adoption of technology, for example our Drones, will further require improved WiFi and connectivity to deliver improved situational awareness to operational commanders remotely, including improvements in our hardware within our Command Support room.

Storage

Protect data where it is vulnerable.

Data needs to be protected from unauthorised access, modification, or deletion. This involves ensuring data is protected in transit, at rest, and at end of life (that is, effectively sanitising or destroying storage media after use). In many cases data will be outside of our direct control, so it's important that we consider the protections that we can apply, as well as the assurances we need from third parties. With the rise in increasingly tailored ransomware attacks preventing organisations from accessing their systems and data stored on them, other relevant security measures need to include maintaining up-to-date, isolated, offline backup copies of all important data.

LFRS currently host several storage platforms across the service including dedicated storage for the service's on-premises database estate as well as unified shared storage for file data and virtualisation. It's designed for maximum reliability, availability, and includes two copies across two different sites for resiliency.

In June 2018 LFRS procured and implemented the service's main storage system called NetApp under a 3+1+1 support and maintenance contract. It is our intention to extended

further as there is no End of Support (EOS) advertised, which will effectively take us forward to at least 2024.

We will:

- Align with the National Cyber Security Centre's 3-2-1 approach for better data resiliency. The '3-2-1' rule is a popular strategy that can be used in most scenarios; at least 3 copies, on 2 devices, and 1 offsite backup. This helps ensure that if one copy is compromised, there is at least one other copy intact.
- Evaluate linking the NetApp storage tier into cloud-based storage such as Microsoft Azure and Amazon Web Services. There will still be a storage presence kept to allow for a controlled migration, which is why we will extend the support of the NetApp into at least 2024. This staged migration will allow us to fully understand any cost implications, which are very difficult to forecast accurately.
- Look to replace the service's three Dell database storage arrays, which become EOS in August 2025 and therefore will need replacing. In 2024 a scoping exercise will be carried out to understand the current storage landscape and where appropriate migrate services into the cloud.

Virtualisation

Government digital directive

The strategic direction across UK Government is now Digital by Default, Cloud First. This requires public sector organisations to consider and fully evaluate cloud solutions first before considering other options.

What is virtualisation:

Virtualisation uses software to create an abstraction layer over computer hardware that allows the hardware elements of a single computer processor, memory, storage and more to be divided into multiple virtual computers, commonly called virtual machines (VMs). Each VM runs its own operating system (OS) and behaves like an independent computer, even though it is running on just a portion of the actual underlying computer hardware.

It follows that virtualisation enables more efficient utilisation of physical computer hardware and allows a greater return on an organisation's hardware investment.

90% of LFRS' servers are virtualised and are located either at HQ, Service Training Centre or North West Fire Control.

We will:

- Over the next five years, deliver a cloud-based option for each server or service replacement to ensure we are aligned with the government's digital directive and

our own Data and Digital strategy. For example, we will consider replacing our Helpdesk software, but as part of that procurement process, we will ensure we evaluate against a cloud-based service first.

Initially there may be a small increase in costs as we run two environments to host servers/services which are on prem and cloud-based, however as more and more services are migrated or built new into the cloud then we can start to decommission the on prem virtualisation stack which will bring down the overall cost of the virtualisation platform.

Mobile Device Management

Migration from AirWatch to inTune

What is a Mobile Device Management?

A Mobile Device Management (MDM) service combines device applications, built-in device management features and infrastructure services. Together, these components allow us to remotely control, monitor, and enforce policies on employee devices.

Why use MDM?

Mobile Device Management is designed to simplify management of devices.

Typical functionality includes mobile device enrolment, the ability to control device configuration, protect data, monitor the status and compliance of devices, and manage enterprise approved apps across a range of platforms and operating systems.

Most MDM services work over the Internet, allowing devices to be managed and remotely controlled wherever they are in the world. This means staff can work off-premises, securely.

We will:

- In 2023/2024 Migrate from our current mobile device management system, Workspace One over to Microsoft inTune to achieve cost savings and align with the Microsoft ecosystem ensuring better protection across our estate.
- Enrol all corporate remote laptops and mobile devices to remain compliant with Cyber Essentials Plus, to increase visibility and therefore security, and to ensure greater support is on offer for staff who are hybrid or remote working.
- Replace any non-compliant mobile devices, such as iPads and iPhones so they meet with the requirements of the Cyber Essentials Plus certification

Telephony Solution

Cisco CUBE replacement

LFRS currently hosts its telephony solution from HQ and Service Training Centre. This solution runs the desk-based Cisco phones, which operate as a traditional office phone solution. It dials internally, externally and internationally as you would expect. Other features such as call forwarding, answer phone services and call handlers that direct options 1,2,3 to other areas of LFRS are also delivered through this solution.

We will:

- Evaluate a solution that allows for the integration of Microsoft Teams into desk-based phones.
- Carry out requirements gathering to ensure all the current features remain available, whilst delivering a solution that compliments remote working.
- Replace the CISCO cube with a modern, supported solution that has the flexibility to meet our needs. The CUBE is an integral part of the current system but may be replaced with another cloud-based solution.

Communications

The Communications Officer's role is to ensure the integrity, performance and availability of the LFRS operational communications infrastructure, in particular the key functional areas of the Airwave radio system and Mobile Data Terminal, in adherence with published and acknowledged best practice standards.

Incident ground radio replacement

The BA Set replacement project is expected to go to tender during 2023/24 ready to purchase 2024/2025 and the Incident ground radio replacement will align with those timings. The BA replacement project is a regional project and the Incident Ground Radio is currently local to LFRS. Currently the purchase for replacement for the Incident Ground Radios is estimated at £230,000.

We will:

- During 2024/2025 replace the Incident Ground Radios in conjunction with the BA Set replacement project. The incident ground radio model that's chosen is a vital component in delivering clear audible voice transmission from the BA teams to the officer in charge, therefore it should not be done in silo.
- Evaluate opportunities for a joint purchase across the region to achieve a cost savings.

On-call Duty System / Day crewing plus alerter replacement

The On-call alerters are still functioning, however there are modern technologies that could enhance this capability making it easier for on call staff to receive notifications about an incident at their On Call station. The expected costs are in the region of £65,000.

We will:

- Evaluate several modern ways to alert on call staff. These are to include text alerts, e-mail and notifications via an app.
- Ensure the final solution is in line with officers' requirements to ensure the maximum benefit is realised.

SAN J Radio Replacement

The Fire Contract in GB is a Managed Service operated by Airwave on behalf of the Home Office. The currently installed MTH800 handheld terminal (SAN C/J) was declared 'End of Service Life' in April 2017 and is currently supported on a "break-replace" service from used stock.

The Airwave National Shutdown Date agreed with the Home Office has extended from 31 December 2022 to 31 December 2026.

Understanding the length of the extension, a spares issue has been identified in supporting the MTH800 post December 2022.

Airwave has a contractual obligation to replace the radio as per the Firelink requirements in the Statement of Brigade Requirements (SOBR) as part of the managed service and to ensure the managed service support continues with the same service levels (SLA) as part of the Firelink contract.

Therefore, a hardware changeover is needed for the SAN C/J devices that were originally provided as part of the Fire contract. No operational risk can be taken through a radio failing on the network so a business case was compiled to upgrade and swap out the existing MTH800 radio to ensure a radio can be put in place with minimal disruption and that will provide longevity to the FRS and is robustly supported from a spares point of view. Alternative options have been reviewed with the Home Office.

Change notices are being agreed between Airwave and the Home Office and technical testing has been completed, including Airwave reference system testing. All tests were completed with no issues found. The Airwave Configuration Team has completed the appropriate fleet mapping work centrally and from an individual FRS perspective there will be no change.

The last part of the preparatory work was to complete a user trial to see if when 'live' on the network if any issues were found or any changes were needed.

The replacement SAN C/J radios (MXP600 radios) have now been ordered to replace the 3,791 SAN C/J devices across the Great Britain for Fire and Airwave is in the process of recruiting a Project Manager (PM) to lead this work.

As part of the 'like for like' replacement of existing installs a new MXP600 device will be swapped for the existing MTH800 by Airwave. The install is not a full install as it was in the Firelink rollout, all wiring and the antenna stays the same for existing installs. The radio cradle and junction box will be swapped out by Airwave and new kit installed as part of the replacement.

We will:

- Assist Airwave with the replacement of the SAN J devices, which is anticipated to commence in January 2023.
- Purchase any additional auxiliary kit which is outside of the contract to ensure full functionality is kept until the introduction of the Airwave/SAN J replacement which is currently estimated for 2026/2027

PSTN End of Life

What the PSTN?

The Public Switch Telephone Network (PSTN) is aging and will reach the end of life in December 2025. The PSTN supports the services tertiary (3rd route) method for mobilising crews.

We will:

- Prepare for ESN which will be utilised as a data bearer for station end mobilisation thereby removing the requirement for PSTN, however if that's delayed then there are several methods that will be investigated in January 2025 to replace those links with more modern methods of communication such as fibre/ADSL/5g.

VMSD/MDT hardware replacement

The current Mobile Data Terminals (Motorola MDT2) utilised within LFRS are becoming end of life. A replacement is required before any potential issues arise.

We have waited until this time so that we can be sure that the new solution would be compatible with the ESN network, which is due to replace Airwave in the life of these units.

The current Mobile Data Terminals are fixed vehicle mounted terminals that allow crews to access risk data and applications which are download to the appliance via Wi-fi when in station and then available when mobile.

The MDT's are connected to the Airwave data network that allows the crew to receive and update mobilising information to from and to Northwest Fire Control.

We will:

- In 2022/2023 implement and validate Mobile Data Terminals which will be compatible with both Airwave and its replacement Emergency Services Network as a bearer.
- Pilot the concept of a second demountable MDT installed in the rear of the appliance, connected to ESN and suitable for both Operational and non-operational activities. (This forms the basis of the Digitising Fire Appliances functionality)
- Continue to work with operational crews and support staff to fully realise all benefits of the rear MDT. This would include options to either add to or replace the functionality on the current iPads on appliances.

The initial pilot is expected to start in February 2023 and follow in March/April with the full roll out across the service, which is to run for 12 months. The budget has been split into two parts, the first at £406,000 for the replacement front MDT units and £254,000 for the additional rear MDTs.

ESMCP/ESN

The Home Office is leading a cross-government programme to deliver the new Emergency Services Network (ESN) critical communications system. This will replace the current Airwave service used by the emergency services in Great Britain (England, Wales and Scotland) and transform how we operate. ESN will enable fast, safe and secure voice, video and data across the 4G network and give first responders immediate access to life-saving data, images and information in live situations and emergencies on the frontline.

This is now set to be delivered in 2026 with the optional extension to 2030. Due to current slippage in the ESN Beta product the focus of work for 2022/2023 is around coverage assurance. In March 2022 LFRS received a new device which allows us to independently assure ESN coverage at our stations and Critical Operational Locations. This new device plots coverage over floor plans and site plans showing what levels of coverage exist. Giving the capability to look at our operational requirements in these areas. This will allow us to understand any gaps in coverage and look at solutions required to fix these ahead of transition. This will assist our acceptance to transition onto ESN in a safe manor.

All our stations and critical working areas will require a ‘passport’ with a high level sign off on coverage acceptance. This will live with the location for the entirety of ESN and provide evidence of coverage and operational requirements should there be any issues in the future.

In the Northwest we have already established strong links with the other Emergency Services ESN teams and regular meet up.

We will:

- Seek assistance from the relevant personnel to complete the coverage 'passports'. There is currently an opportunity to update our Critical Operational Location list held with the programme the service may wish to update.
- Towards the end of 2022, we will be looking at the resilience of the ESN network should we be put in a national grid outage or suffer damage during storms. Plans will need to be reviewed on what coverage would be available during these times and if it would be sufficient for our operational requirements.
- Continue to work closely with the Home Office to help prevent any future project slippage where we can.
- Look to become early adopters of ESN, even if this is just for piloting to ensure coverage assurance and to also assist with buy in from other FRSs.
- Migrate to ESN once it has been approved and is fit for operational purpose, which is estimate currently to be 2026, however this could extend to 2030.

Cyber Security

The security landscape is rapidly changing, and we need to evolve at pace to reduce the likelihood and impact of a cyber-attack.

The following Cyber Security section and subsequent longer terms objectives have been identified for three main reasons.

1. The threat landscape has changed significantly, which has been witnessed globally, regionally and across multiple emergency services and local authorities.
2. Best practice standards set by the National Cyber Security Centre (NCSC) have changed according to that change in the threat landscape, which means it's far more challenging to remain compliant.
3. The necessary adoption of cloud-based services and remote working has effectively tippled the services attack vector.

We have been awarded both Cyber Essentials and Cyber Essentials Plus accreditation, which are government backed schemes that involve external auditing of IT systems. This certification also allows for better collaborate with other authorities such as the Lancashire County Council and Lancashire Constabulary as there is a growing requirement to be security compliant.

Cyber Essentials:

Cyber Essentials is a minimum standard of cyber and information security that your organisation should be able to demonstrate to customers and business partners.

The requirement to demonstrate that your organisation is doing what it feasibly can to keep data safe is also a key principle of the UK GDPR (Article 5) and is therefore a legal requirement under data protection legislation.

Certification also comes with commercial benefits, with prospective customers (especially government clients) seeing this certification as a mandatory requirement to engage a new supplier.

Cyber Essentials Plus:

Cyber Essentials Plus still has the Cyber Essentials trademark simplicity of approach, and the protections you need to put in place are the same, but for Cyber Essentials Plus a hands-on technical verification is carried out.

The LFRS Cyber Security Strategy is underpinned by the adoption of the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF), which is the assurance framework for local Government.

We have combined and prioritised the "10 Steps to Cyber Security" identified by NCSC down into four distinct categories.

Engagement and training

People should be at the heart of any cyber security strategy. Good security considers the way people work in practice and doesn't get in the way of people getting their jobs done. Supporting our staff to obtain the skills and knowledge required to work securely is often done through the means of awareness or training. This not only helps protect LFRS, but also demonstrates that we value staff, and recognise their importance to the service.

We will:

- Work closely with DTX and Corporate Communications to publish changes to working practice and engage closely with staff members to reenforce a positive cyber security culture.
- Delivery annual cyber security LearnPro modules to keep staff members up to speed with the latest security threats.

Future enhancements

There are a few different ways in which we need to fortify ICT defences, starting at the perimeter. Investment in Firewalls with tools that include next generation detection and prevention, which include automation that allows them to learn what's safe and what isn't to proactively protect the service.

What is a Firewall?

A firewall is a device that filters and determines the network traffic that is allowed to go to or from other sections of the network and/or Internet.

Firewall technology has advanced over recent years to help mitigate more of the wide spread of potential threats. These offer us greater protection, enhanced visibility and alerting to what is happening on the perimeter and on our network. These new firewalls are called next generation NGFW.

The global pandemic and current geopolitical landscape have caused great issues with supply chains across all sectors. With all forms of technology becoming advanced, a global computer chip shortage has been exacerbated due to this, with vendors struggling to meet demand and imposing long wait times for hardware. This project along with our Wi-Fi estate, which is also becoming end of support is not immune to this, however there are vendors that offer a quick turnaround that will be evaluated.

We will:

- In 2022-2023 we will carry out a procurement exercise which is expected to cost in the region of £200,000 to purchase the Next Generation Firewall. This Firewall will be in place until at least 2027, which is the duration of the expected contract.
- Remove the issue with chip shortage by using an industry leader which is not reliant on chip sets from overseas.
- Install and enhance the next generation security features to allow for better automation which will mean less reliance on manual intervention.

Microsoft 365 License Model

Currently the service purchases a M365 E3 Premium 1 license for each staff member and in June 2022 an elevated security license was purchased which gave the us Microsoft Defender for Endpoint. This aids with the security and management of the mobile estate as well as providing enhanced threat analytics.

The NCSC best practice guides point to regular desk based BCP exercises.

We will:

- Renew the Microsoft license using the most cost-effective model, which will include evaluating options for a joint procurement.
- Develop awareness of the features that the licenses bring across the LFRS and support for the governance and use where possible.
- Continue to evaluate the threat landscape and propose changes to the license model.
- Collaborate with LFRS Business Continuity and Emergency Planning Officer to ensure cyber threats are included within the scope of BCP exercises and that desk-based scenarios are played out to closely simulate an attack.
- Look at achieving a license model that is both cost effective and rich in security features.

How do we deliver this Plan?

The 2022-2027 ICT Plan maximises the effectiveness and efficiency of our workforce to ensure the best possible service and levels of engagement for our communities and it ensures a strong foundation is in place that supports and underpins the delivery and development of the service's Data and Digital Strategy.

It will be monitored via the ICT departmental plan with key items being referenced in the Annual Service Plan, with each major project featuring in the Capital Programme (Appendix A)

Individual checkpoint reports will be delivered via our Business Process Improvement Programme Board (BPIP) to ensure any risks to projects are highlighted and recorded, and that the projects meet their projected completion time scales and associated costs.

Appendix A

Capital budget requirement 2023/24-2027/28

	2023/24	2024/25	2025/26	2026/27	2027/28
	£m	£m	£m	£m	£m
Replace Existing Systems					
Pooled PPE system	-	0.100	-	-	-
Stock Management system	-	0.100	-	-	-
Asset Management system	0.100	-	-	-	-
HFSC referral system	0.100	-	-	-	-
Fire Risk Management System	0.100	-	-	-	-
Rota management package (WT/On call)	-	0.100	-	-	-
Storage Area Network	-	0.200	0.090	-	-
GIS Risk Info	-	0.100	-	-	-
WAN	-	-	0.450	-	-
IRS/MIS	-	-	0.050	-	-
Firewall	0.235	-	-	-	-
Wi-Fi	0.135	-	-	-	-
New Operational Communications					
Digitisation of Fire appliances - additional VMDS units	0.254	-	-	-	-
Replace Operational Communications					
ESMCP (Airwave replacement – assumed funded by grant)	-	-	1.000	-	-
Incident Ground Radios	0.230	-	-	-	-
UPS	-	-	-	-	0.060
Total ICT Programme	1.219	0.500	1.690	-	0.060

Lancashire Fire and Rescue Service

Lancashire Fire and Rescue Service (Official)

LancashireFRS

@LancashireFRS

LancashireFire

For further information on our services please visit

www.lancsfirerescue.org.uk