



# Northamptonshire Fire and Rescue Service

---

## ICT Strategy 2019 – 2024

### Document control

Version	Date	Issued to
Draft Vers 0.2c	28/05/2019	D Dovey, R Porter, P Meredith,
Draft Vers 0.3	21/06/2019	D Dovey, R Porter, P Meredith
Draft Vers 0.4	08/07/2019	D Dovey, R Porter, P Meredith, S Iddon, M Scoble
Final Vers 1.0	02/01/20	D Dovey, S Iddon, P Bullen
Final Vers 1.1	30/01/20	D Dovey, P Bullen

# *Making Northamptonshire Safe*

## **Contents**

NFRS Strategic Objectives: .....	3
1. Introduction .....	3
2. Governance.....	3
3. Scope.....	3
4. Principles.....	4
5. Strategic ICT Objectives .....	4
6. Current position, Key Issues and Activities Required.....	4
Strategic Objective 1.....	5
Strategic Objective 2.....	6
Strategic Objective 3.....	8
Strategic Objective 4.....	10
7. Capital Funding Requirement.....	<b>Error! Bookmark not defined.</b>
APPENDIX 1 .....	<b>Error! Bookmark not defined.</b>

# *Making Northamptonshire Safe*

## **NFRS Strategic Objectives:**

- Keeping our communities safe and well
- Keeping our staff safe and well
- Making the best use of our resources

## **1. Introduction**

- 1.1 The purpose of this ICT strategy is to provide a framework to help ensure a legally compliant and fit for purpose ICT environment that supports the requirements of NFRS operational, support and administrative functions, enables delivery of the strategic objectives within the Fire and Rescue Plan and IRMP and provides for safe systems of work.
- 1.2 The strategy will inform and underpin the NFRS Capital Programme.
- 1.3 It is recognised that the ICT strategy and plan will be subject to review and change as the “enabling services” project delivers the desire for a joint ICT function and capability.

## **2. Governance**

- 2.1 The ICT Strategy is ‘owned’ by the Chief Fire Officer and will be reviewed by the Fire Executive Group (FEG) annually.
- 2.2 Any financial implications must be agreed by the Chief Finance Officer and included within the MTFP.
- 2.3 Once agreed, the ICT Strategy will be submitted for approval and adoption by the NCFRA

## **3. Scope**

ICT is a critical component in enabling NFRS to deliver services to meet the statutory obligations placed upon the NCFRA through the Fire and Rescue Service Act 2004 and related legislation. With the growth in the role of ICT and the ever increasing integration of systems and processes, there is no longer a clear line between front-line and back-office ICT systems, with all aspects of ICT having a role in supporting front-line service delivery and in enabling continuous improvement.

The scope of this strategy covers the following areas:

- Mobilising systems
- Wide and local area networks
- Business systems (hardware and software)
- Telephony (fixed and mobile)
- Radio Communications
- Support and Maintenance
- Software Application Systems both Fire Service specific and ‘desktop functions’
- Cyber security and relevant accreditations such as Airwave Firelink, ESN ESMCP & PSN

# *Making Northamptonshire Safe*

The move of Governance of NFRS in January 2019, from the County Council to the Northamptonshire Commissioner Fire and Rescue Authority (NCFRA), has opened the way for wider and deeper collaboration and integration, particularly between Northamptonshire Police and NFRS. ICT is a key enabler to collaborative working and the opportunities for aligning or integrating systems and software must be a primary consideration before significant infrastructure upgrades or changes during the life of this strategy are enacted. A review of respective ICT roadmaps will help align infrastructure and software development plans, this should be undertaken as soon as practicable as in doing so, will develop milestones for achieving integrated services for the benefit of the community and each organisation.

## **4. Principles**

The ICT strategy is driven by the following overarching principles:

- Operational effectiveness
- Safety
- Efficiency
- Legal compliance
- Value for money
- Protect the environment

## **5. Strategic ICT Objectives**

This strategy and supporting action plans will work to deliver the following strategic objectives:-

1. To work with Emergency service partner agencies to seek out joint initiatives, opportunities for collaboration and integrate systems and supporting functions to ensure effectiveness and provide value for money.
2. Develop ICT infrastructure to improve data sharing and collaborative opportunities with partners, utilising cloud functionality to access secure local data
3. Ensure ICT services remain safe, secure and fit for purpose through planned and incremental replacement and upgrades without disruption to Service Delivery
4. Introduce and develop electronic ways of working to improve capacity and capability in delivering prevention and protection activities.
5. Increase the opportunity of remote and mobile working by the continued roll out of mobile technologies and VPN connections.

## **6. Current position, Key Issues and Activities Required**

This strategy constitutes a continuation of the direction of travel of recent years wherein completed actions to date are already providing benefits in support of the strategic objectives and are providing improved organisational assurance and user

# *Making Northamptonshire Safe*

experiences. The Microsoft licencing model has already been changed to allow for the Microsoft Office E3 365, having already implemented and made use of cloud technology. The following provides a brief overview and signposts key issues and required actions during the life of this strategy.

Whilst not specifically referenced in each section below, it can be assumed that any review of structure, skillsets, infrastructure or refresh of these systems and /or applications will need to take account of the strategic collaborative/integrated intent of the 'enabling services' work streams.under development within the OPFCC at the time of writing.

## **Strategic Objective 1**

**To work with Emergency service partner agencies to seek out joint initiatives, opportunities for collaboration and integrate our supporting functions to ensure effectiveness and enhance value for money.**

- In recent years the growth in shared estates between NFRS and NP has necessitated ICT network design and restructuring. It is anticipated that further sharing of estate will occur during the life of this strategy and with that, opportunities for closer collaboration and integration on ICT will emerge.
- NFRS currently operate a shared mobilising system (and associated infrastructure) with Warwickshire FRS, enabling interoperability, efficiency and resilience in this statutory function. The existing contract (5yrs) will run until 2023/24 wherein a 2 year optional extension can be employed. The future options for fire control will be explored with NCFRA during the life of this strategy wherein consideration will be given to all options including further co-location and/or integration with Northamptonshire Police. The ICT roadmap will be reviewed to reflect any decisions that emerge in this respect. Costs for any future approach will need to be fully scoped and will be dependent both upon the system requirements and whether the control room moves to a new location. As such the costs included within the plan in appendix 1 can only be indicative at this time.
- NFRS will continue to engage with the National ESN/ESMCP project for which new ESN standards are being applied that will enable full main-scheme radio interoperability.
- NFRS will continue to actively work towards partnership working agreements and to have the infrastructure and network certification that will allow data sharing facilities and will put in place user maintenance systems that will be compliant to Government security standards including password managed individual log-on and/or other dual authentication security functionality that will ensure that fire and rescue is a trusted partner for data sharing and network access.

# *Making Northamptonshire Safe*

- NFRS maintain and fund a number of common non fire service specific products in the IT area, such as Microsoft licencing, Cisco network, Virus control and reporting tools. Within the life of this strategy, opportunities will be sought to combine contracts and obtain discounts due to higher volumes.
- Currently, NFRS run small support teams with a breadth of experience and knowledge supporting specialist and specific fire service systems, however there is a potential for 'single points of failure'. Opportunities will be sought through collaboration and/or organisational restructure, to increase capacity in support of key functions, with the additional advantage of maintaining skills by training and pro-active succession planning

## **Strategic Objective 2**

**Develop our ICT infrastructure to improve our data sharing and collaborative opportunities with partners, utilising cloud functionality to access secure local data**

- NFRS has a Virtual Private Network (VPN) that links to all NFRS locations, Deploying Secure boundaries using DMZ architectural design within MPLS network this ensures that fire and rescue service data is secure and managed. The overarching objective remains to ensure best value for money while at the same time ensuring that capacity is maintained to meet the needs of the service.
- The increasing complexity of networks and additional demands of data security will require the deployment of integrated management tools and possibly 24/7 managed services. These will require dedicated specialist personnel which currently fire and rescue service are not able to fully provide. Network support will require constant review as tools are developed to meet the increasing and changing threats levels posed and with that implement the technologies required to counter these threats. Fire and rescue recognise that partner working must be based upon having in place trusted network infrastructures and supported by procedures that are both robust and effective.
- Various contracts are in place to support these objectives and contract review is an essential part of the strategy to challenge suppliers and review partnership objectives. By reviewing networks costs, capacity and functionality with partner organisations NFRS would look to both reduce cost and increase capacity.
- NFRS currently run two, small centres based upon W2012 R2 virtualised clusters. These hold relative small volumes of data, but still require the overheads of data security, environmental resilience, performance and functionality regardless of the volumes involved. With funding pressures recognised as an on- going issue we need to reduce our cost / data volumes ratio, while at the same time managing technology change and increased capacity requirements.

# *Making Northamptonshire Safe*

- It is recognised within the strategy that the period up to 2032 will continue the trend from desk based On-premise data processing to mobile devices working in the Cloud, with data access becoming more complex, moving from single source database records to analytical data processing gathering together multiple data sources. This will challenge the role of ICT as hardware continues to become less problematic but the ability to deliver integrated data solutions, will call upon new skills sets from within the ICT Department.
- ICT will continue to develop partnership working and participate in user forums as a means of seeking out best practice. It is the intention of the service to ensure that we are classed as excellent users of any software applications that we use, with the stated intention to obtain the maximum benefit possible from the software; by being aware of and adopting best practise from peer organizations. To achieve these aims fire and rescue employ ICT project officers with the specific role to implement best practice solutions into fire and rescue. Currently the focus is on Fire Control systems, Human Resource and Rota Systems, Data Management and Asset Management Systems, in addition to daily support functions. Via partnership working and collaboration, fire and rescue will look to strengthen ability in these areas by providing additional resource, by not 're-inventing the wheel' and finding resource time for successful completion and not leaving 'loose ends'.

ICT Infrastructure activities will include:

- Continue to implement hardware lockdown procedures whereby all laptops are upgraded to Windows 10 with encryption applied. Devices to be locked by network management tools and policies, to control the use of memory sticks and other uncontrolled devices. All memory sticks will be encrypted
- Continue to create improvements to the infrastructure where required, including development of the second data centre at Daventry and the development of the Chelveston training facility.
- To maintain network certificates and password procedures, in keeping with PSN best practise and to further explore the most practical means to deploying these recognising that single sign-on and a properly managed Active Directory environment, provide for a better user experience than maintaining multiple user Ids and passwords
- Continue to implement DHCP Fail-over and to run fall-back DR exercises using replicated data at the second cluster at Daventry. The current procedures in place do not meet Government best practise with recovery procedures subject to manual intervention and with a limited capacity to run a full Disaster Recovery for an extended period of time
- Develop and support the fire and rescue training facilities at both the Daventry Command Development Centre and the Chelveston Fire Behaviour Training Centre. ICT will provide and support standard IT and network facilities and also provide assistance with the integration of

# *Making Northamptonshire Safe*

specialist software and equipment. These integration data gathering functions, also apply to other areas including fleet management, health and safety and asset management

- Continue to develop and upgrade the fire and rescue service SAN storage to maintain capacity and functionality that will also utilize better maintenance tools which are available within new technologies being developed. Fire and Rescue recognise that over the period of this strategic review, data volumes will continue to grow at 20% or more per year and increasingly that data will be required to be available off network via Cloud based functions. The costs of managing this change and maintaining effective systems will be an opportunity for better resourced partnership working solutions.
- To review annually the Business continuity plan for ICT including both Fire Control Mobilising systems and administration systems such as the VoIP telephony systems. This review will require the possible upgrade of the Cisco CUCM as the network support reaches end of life, by an alternative telephony system that combines both landline and mobile telephony, while also recognising the development of Skype for Business (or other IP solutions) as a viable alternative to conventional telephony systems

## **Strategic Objective 3**

**Ensure ICT services remain safe, secure and fit for purpose through planned and incremental replacement and upgrades without disruption to Service Delivery**

- It is the intention and strategic objective of fire and rescue that all ICT equipment will remain fit for purpose, relevant to the needs of the service and in a supportable state to enable maintenance to ESN/ESMCP standards. The equipment deployed and supported must be directly contributing to the improvements and the effectiveness of fire and rescue services operations, whether in mobilising emergency response or in the areas of protection and prevention. This will extend to a programme of desktop hardware refresh, the network environment and also the application software products deployed to support fire and rescue daily business. By implementing a constant programme of refresh the strategic objective of obtaining maximum benefit from the investment made by fire and rescue service, will be fulfilled.
- Specific mention must be made to the ESMCP programme and the associated PSN/ESN network standards required, that will increasingly play a part in the workload of ICT in the period of this strategic period. Up to 2022 (current national project timeline), the Airwave system will need to be maintained via the Firelink accreditation process that currently includes Annex A – network environment, Annex C Intrusion and network boundary protections, and with separate declarations required to our partnership



# *Making Northamptonshire Safe*

organisations (Warwickshire FRS and Royal Berkshire FRS) via Interconnection Communication Documents (ICD's). This level of activity will be duplicated for ESN as the standards for ESMCP are developed. It is a strategic objective that fire and rescue do obtain ESMCP accreditation.

ICT Upgrade activities will include:

- Achievement and maintenance of network certification (ESN/ESMCP) to the required Government standards, the compliance to be supported by fire and rescue policies and procedures that achieve certification in support of ESN/ESMCP. Until such time as ESMCP is fully deployed as the sole means of blue light communications, fire and rescue will maintain compliance to the Firelink Airwave systems
- To continue to implement Cyber Protection and to ensure the maintenance of Firewalls and other security network infrastructures. Fire and rescue recognise the cyber threat to the operation of daily business is both real and dynamic requiring constant vigilance as part of a recognised strategic objective and with sufficient and competent personnel to support this function. We will also look at partnership opportunities to increase expertise, ensure procedures are robust and resilient, and are cost effective.
- To develop network tools; ensuring that ICT personnel are trained and competent in the use of the software tools deployed within the service and that contracts and licences are maintained in support of this objective with the appropriate third party security system providers
- Ensure that data held within the FRS corporate systems is secure with the appropriate user permissions. Using Microsoft Active Directory software is the key security authentication, fire and rescue will look to deploy federated Active Directory with partner organisations while ensuring all NFRS computer users have a unique and password maintained log-on
- It is NFRS policy to maintain and support the use of secure email and secure large file transfer where required for partnership working. This will require establishing procedures for the use of secure email and creating the correct levels of authentication for those fire and rescue service personnel who require secure credentials specifically for encrypted communication
- To annually run an IT Health Check and penetration test that will confirm the NFRS systems are being correctly maintained and that any daily business activities or project based enhancement have not compromised the security of the fire and rescue network. Any required measures recognised will be implemented to ensure that compliance is maintained to the required security specifications in force at that time.
- It is the intention of NFRS to develop and implement the use of secure printers that will ensure all personnel are following procedures for

# *Making Northamptonshire Safe*

confidentiality relating to hard-copy documents (there are further objectives within the strategy to reduce printing at part of Strategic objective 5)

- To review and develop resilience within the network infrastructure, including use of a second Airbus Gateway and designing auto fail-over from 100Mb Daventry to Leamington Spa circuit to the NFRS MPLS network (which has a link into the Leamington Spa Control Room). This activity will also support the potential use of a Single Control Room and/or further integration with Northants Police at the 999 call centre level. All of these activities and the areas outlined above will be designed and implemented under change control procedures with the express purposes of maintaining daily business and recognising any potential risk associated with the change.

## **Strategic Objective 4**

### **Increase the opportunity of remote and mobile working by the continued roll out of mobile technologies and VPN connections.**

Recent years has seen desktops replaced by laptops and tablets for personnel who frequently work at more than one site; laptops replaced by tablets for personnel whose role required desktop functionality outside of the NFRS network and that all service issued mobile phones are now smart phones with email/ internet capability. There is an overall aim to improve and enhance the capability of the NFRS software applications by supporting the workforce with mobile working and next generation working processes.

Our Mobile Technology Roll-out will include:

- We will develop wireless at the incident ground, supported by security VPN tunnelling, while ensuring that fire and rescue systems have the capability to work in conjunction with the JCU and other partner facilities.
- We will develop our vehicle based systems which currently have a single mobile data terminal which is locked down by Airwave certification to mobilising processes.
- Expand the use of tablets and development of software in the areas of inspections and other community activities. This will require investment in both software and hardware with the stated benefits being data entry at source, avoiding dual data entry and queries, resulting in overall faster completion of the required process.
- We will ensure that our desktop software remains current by upgrading to Microsoft Office 365, further developing the application of Cloud based technology... We will actively promote the use of Skype for Business and the use of instant messaging and video conferencing
- Undertake a review programme to confirm how best to apply new technology including wall display boards; integration of new software and hardware; conference room booking, other booking functionality such as loan equipment or

## *Making Northamptonshire Safe*

vehicles, integrated access control and the use the smart devices for identification and/or log-on to fire service facilities.

- Over the next few years hard copy form will be replaced by implementing electronic forms. This is in support of objectives to reduce printed hard copy and by this process to create greater efficiencies. The initial aim is to replace where applicable, paper versions of the FB forms, standard letters and other documents with electronics forms with appropriate workflow and security. This will generate business process management or workflow process and will need to be assessed in conjunction with other stated aims for the upgrade to SharePoint 2016 and the potential use of CRM as an alternative to our current protection and prevention systems.

# *Making Northamptonshire Safe*

## **Appendix 1 – ICT replacement programme**

The plan that accompanies this strategy below is based on current knowns and operating model. It is envisaged that the ICT delivery plan will change in line with the desire for a Joint ICT team and Joint ICT functionality which is to be delivered via the “Enabling Services” project.

Whilst recognising that the plan below is cross cutting in terms of delivering the strategic objectives the priorities are designed to predominantly deliver the following:

- Priority 1 - Essential for core functionality & legal compliance
- Priority 2 - Maintain service delivery
- Priority 3 - Improve service delivery

Some of the items on the plan will be capital and some revenue. Capital items will form part of the overall Capital plan for the service whereas revenue will be identified within an appropriate revenue budget or ICT revenue reserve.

The capital plan that accompanies this strategy can be found here.

[\(Insert link to capital plan\)](#)