IT Strategy

2020- 2022

CONTENTS

INTRODUCTION

The Digital Landscape is a fast growing area, its constantly changing and evolving and it is the role of any IT department to embrace the technology and adapt it for use for the organisation. New fields are emerging such as cloud, robotics, system self-learning and virtualisation all of which can be enhanced to provide a better service to the public of Cheshire.

Collaboration and interoperability are other factors that this document will address. Changes in technology were one of the key drivers in reforming the data protection law, leading to the introduction of the General Data Protection Regulation (GDPR) in May 2018. The GDPR contains new provisions to allow us to better protect our data by design.

The advances within this document will not come at the expense of data protection and privacy rights – our approach to technology will bring GDPR and innovation together to create true trust and data integrity and confidence. Technology advances are therefore viewed by Cheshire Fire Services both as a risk and an opportunity.

We will continue to provide a service to Cheshire Fire and Rescue including creating new systems such as SAFFIRE, providing technology to introduce more mobility, the delivery of a new command vehicle and supporting the technological infrastructure. We will also work with you to provide the best customer service so that issues are resolved quickly and staff can continue with their day to day roles.

KEY PRINCIPLES

In order to deliver our strategy we will be working on 4 key principles, support, transform, service delivery and cyber security. All of these principles combined will provide the organisation with an effective and efficient IT department and help deliver projects. They will also support Cheshire Fire's Core values.

The 4 key principles are:

SUPPORT

SERVICE DELIVERY

CYBER SECURITY

TRANSFORM

SUPPORT

To deliver this, it is essential that we give our staff the right tools to deliver this effectively and efficiently. It is also important that we give IT support and customer services staff training and information on this new technology so that we can provide effective solutions to issues and problems.
As well as supporting our own staff, it is important that we provide the correct information to the end user especially with the type of data protection risks their use of technology may be subject to.

Ensure effective education, awareness and welfare for all our staff.

We will develop training programmes for IT Services staff that will develop their technical knowledge and understanding at a level appropriate to their role. This training will aim to develop core knowledge of how essential technologies work and further learning on new and emerging technologies. This will also include technology briefings for the senior leaders within Cheshire Fire.

We would also like to attract, develop and maximise retention, engagement and productivity of a high-calibre IT professional workforce through inclusive, effective leadership and investment in succession planning and employee development.

Provide effective guidance to Cheshire Fire about how to address data protection risks arising from technology.

As well as developing guidance to support the technology priority areas we have identified, we will update our existing technology guidance to reflect the requirements of the new provisions in the GDPR, the Directive on security of Networks and Information Systems (NIS) and ePrivacy Regulation. We will promote the use of data protection design by default, and demonstrate how these contribute to UK data protection. We will also write new guidance about these provisions in the GDPR. We will publish a report on 'lessons learned' from cyber breaches reported to the ICO and technology issues emerging from Data Protection Impact Assessments annually.

Outcome

- We will keep Cheshire Fire informed about emerging risks and opportunities arising from technology and cyber in an appropriate and timely manner. This will include blogs, social media and webinars.

TRANSFORM

In order to support Cheshire Fire, we will introduce new technology to support staff to deliver the best service to our communities.

End User Experience

Optimise the end user experience with data, access and services while providing cost efficiencies and workforce productivity. People are able to interact with the world around them in new ways due to the ubiquity of network connectivity and the proliferation of smart devices. It is also important that we give the end user the easiest way in which to complete their tasks be that through automation or simplifying data entry.

Data Analytics

Everyone wants real-time data and analytics. Our goal is to make that type of technologies available that will provide the right information, to the right people, at the right time, in order to help perform with greater efficiency, productivity, and safety

Interoperable Technology

To develop interoperable technologies that enable detection of and resilience against threats. We will focus on the new Emergency services Network (ESN) solution for the country's new radio and mobile data network, as well as a working collaboratively with Cheshire West and Chester and Cheshire East on the new county wide area network. This represents a unified effort across the enterprise to assess gaps and obstacles, and develop a roadmap to successful interoperable communications.

Information Sharing

The department will continue to grow its information sharing capacity by adopting a collaborative approach; utilizing shared technology platforms; embracing a customer-focused information delivery model; and integrating GDPR into technology solutions. This will include evolving an information sharing segment architecture; developing agile and mobile information sharing platforms and applications; and establishing strong governance enforceable policy, and clear standards.

Enable end to end delivery of mobile solutions

The department is advancing with its mobile computing environment to enhance mission effectiveness, improve the end user experience, and enable cost reductions in both hardware and device support. The transformation is already underway and will require strong collaboration with IT stakeholders and partners. As technology evolves, IT Services will move beyond its current capabilities to provide additional features and services to the mobile end user device and application computing environment.

Outcome

To support the above we will;

- Improve user experience by providing the correct IT resources including network, systems, data and people to complete tasks efficiently and effectively.
- Continue to improve mobility while making it interoperable and secure.

SERVICE DELIVERY

Customer service is at the forefront of what we deliver in IT Services. In order to deliver that, we need to put the right infrastructure in place that is cost effective whilst still delivering what the organisation needs particularly around working with outside partners who provide our technology. We are also committed to continuous improvement so that what we deliver is the best it can be.

Effective Service Level Agreements

We will enhance IT Services capabilities and our support partners by ensuring operational excellence, framed by service level agreements and delivery that meet the requirements of the Force digital strategy.

Improved Budgeting

Creating a customer service model to improve delivery of high quality IT services, including transparent expenditures while advancing the adoption of scalable, flexible, cost-effective, accessible services through enterprise and brokered service offerings. The department will continue to consolidate legacy contracts and systems, and increase the use of cloud and commodity services.

Moving to the Cloud

Continuing to move the organisation into the next generation of Enterprise Cloud Computing that facilitate timely provisioning and delivery of services.

Workflow analysis

Promote effective, timely, and informed decision-making through analytic, knowledgebase technologies and workflow process re-engineering. IT Services will continue to analyse and redesign its workflow in order to optimise end-to-end processes and to make better informed, unified, and expedient decisions.

Outcomes

To deliver the above we will;

- Provide an IT service in accordance with ITIL principles
- Support the transition from traditional service provider models to new broker models such as cloud computing
- Deliver effective and efficient service level agreements with partners and hold them to account if they are broken
- Develop and employ technology tools to support and automate the integrated collection of key program information for critical analysis and enhanced decision-making across the enterprise

CYBER SECURITY

Protecting the technology infrastructure is an essential in IT. A key part of our strategy to make our data and information safe and secure whilst also adhering to GDPR so that inappropriate audiences do not access sensitive information. We also want to protect the force from any data breaches that may be subject to scrutiny from the Information commissioner.

Adhering to Data Legislation

Adopt risk-based common policies and best practices that meet Data Protection legislation to effectively eliminate vulnerabilities and mitigate cybersecurity threats.

Assure Technology and new systems meet Best Practice

All technology and systems introduced should be done in a consistent manner. National Cyber Security Centre Best Practice and NIST/ISO 27001 control frameworks will be used to help protect our data. New systems may be either hosted on-site or in the cloud.

Improving Network Security

Enhance the Cheshire Fire security model by moving to a next-generation network security architecture that accommodates public and private cloud services, improves on current network and integrates new technologies.

Outcome

In order to protect the organisation from threats we will;

- Assure new systems and processes to maintain Information Security
- Raise awareness with staff of the dangers and risks that are prevalent in our modern society
- Follow best practice guidance and industry standard control sets, such as NIST and ISO 27001
- Continually review our security products to ensure they remain fit-for-purpose
- Work with security practitioners to ensure common practices are adopted and maintain
- Understand how security best practice can assist in reducing cost to the organisation.