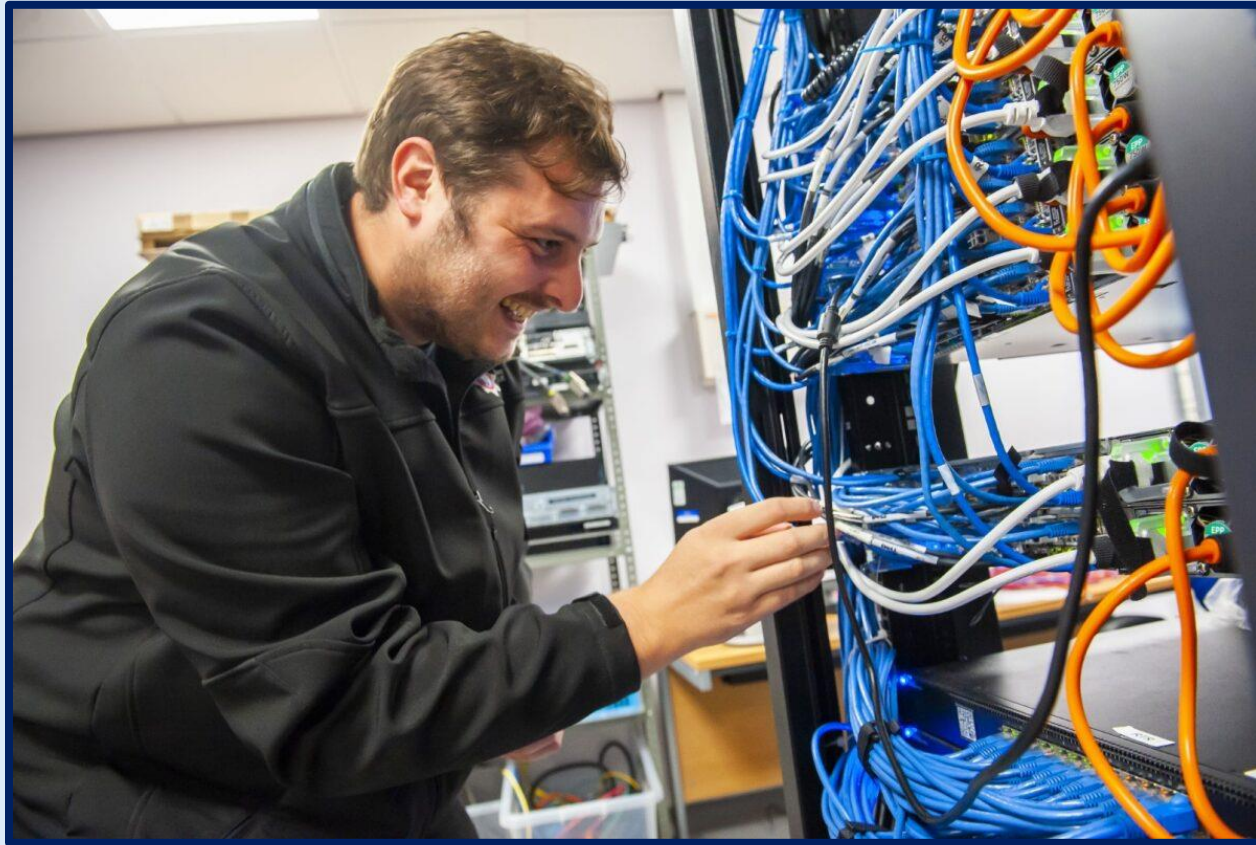**DORSET & WILTSHIRE**
FIRE AND RESCUE

Data, Digital & Technology Strategy 2024-28

PASSIONATE ABOUT
CHANGING & SAVING LIVES

About this strategy:

To help make Dorset and Wiltshire a safer place to live, work or visit, we need to ensure that all our efforts and resources are focused on having the right people in the right place, at the right time, with the right skills and equipment to prevent, support and respond to emergencies when they happen.

To help guide our thinking, and to keep ahead of an everchanging world, we regularly review both our external operating environment, as well as carry out an internal analysis of where our Service needs to be. This is delivered through our Strategic Assessment of Risk (SAR). Our SAR supports the development and review of our strategic plan, which we call our Community Safety Plan, along with the delivery of our five organisational strategies, which includes this Data, Digital and Technology Strategy.

The delivery of this Data, Digital and Technology Strategy therefore sets out the areas of focus for the next four years, and sets the direction for our use of data, digital and technology. This strategy also underpins the Government ICT Strategy and supports both the Networked Fire Control Services Programme (NFCSP) and the Emergency Services Mobile Communication Programme (ESMCP) and subsequent Emergency Services Network project (ESN).

This strategy is translated into an on-the-ground action at department, station and team level through our Service Delivery Plan, which is underpinned by a comprehensive performance framework. This helps us to remain an efficient and effective Service, plan for the future, meet our changing need and ensuring the delivery of our key priorities.

Purpose:

The purpose of this strategy is to set out a long-term pathway to deliver against the ambition set out the Community Safety Plan and the policies agreed by the Authority. In developing this document, we have considered the:

- problems and critical issues we need to respond to
- policy objectives set out by the Authority
- Service priorities and our capacity to achieve them

All five Service strategies are interlinked across all of the Service's directorates; therefore, their delivery is overseen by the members of the Cross Directorate team. Each strategy is led by a key director and for this strategy the Director of Corporate Services has responsibility. Delivery progress will be monitored through the Service's performance management arrangements, ultimately reported through to the Strategic Leadership Team and the Fire Authority.

These symbols highlight where we have a focus on Equality, Diversity & Inclusion and Environmental Sustainability

Strategic issues and challenges
From looking at our Strategic Assessment of Risk we expect:

- there will be financial volatility and uncertainty for the foreseeable future
- there is a global and national focus for organisations to ensure environmental sustainability
- there is a need to invest in the sustainability and resilience of Information and Communication technologies
- there is a need to adapt to an ever-evolving cyber security landscape

The strategic focus for Data, Digital and Technology, for the Service, over the next four years will be to:

- maintain and strengthen information governance and security arrangements
- ensure resilient operational communications and advancing incident ground technology
- maintain and strengthen a resilient ICT infrastructure
- drive forward digital transformation to use technology for improved user experience and efficiency
- further strengthen the use of business intelligence and quality data management for improved data led decision-making
- focus on the health, safety and wellbeing of our staff to ensure an open and positive organisational culture
- maximise the use of technology to support the Service's budget reduction by £2.5m over the next 2 years to improve its future financial sustainability
- use data and technology to further strengthen our productivity, and value for money including better aligning our resources to risk and demand

Information governance and security
Where are we now:

- information governance impact assessments in place to ensure privacy and security is embedded at the design phase
- compliance with information legislation such as General Data Protection Regulation (GDPR), Freedom of Information Act 200 (FOI) etc.
- cyber action plan being delivered to achieve compliance with National Cyber Security Centre's (NCSC's) Cyber Assurance Framework and Cyber Essentials
- annual ICT health check conducted, and changes implemented to accommodate the changing cyber landscape
- cyber incident response plan in place and regularly tested
- cyber security central to internal audit programme

Where will we be in four years:

- fully embedded information governance arrangements, aligned to the National Fire Chief Council's (NFCC's) data management standard
- compliance with the NCSC's Cyber Assessment Framework and annual accreditation to Cyber Essentials
- have a cyber aware culture

How will we get there:

- we will continually monitor and further strengthen our information governance and security arrangements, to ensure we remain resilient against evolving cyber threats, legal compliance and national guidance

Digital transformation
Where are we now:

- making the most of cloud technology through the use of Microsoft 365 to help automate and streamline our management and administration that reflect new ways of working
- data migration to SharePoint

Where will we be in four years:

- embedded cloud first strategy for internal and third-party systems
- improved user experience supporting 'the once only' principle
- digital by default fully embedded that supports the principles of flexible and smarter working
- improved processes making increased use of technology

How will we get there:

- migrate all legacy systems to Microsoft 365 or a third-party software solution including Estates, Health and Safety, HR Management Information System
- maintain and develop skills in Microsoft 365 and future technologies
- increase use of national procurement frameworks for purchasing technology, to achieve value for money and support sustainability
- develop an App based approach for access to information supported by hardware to meet user needs
- monitor usage of Microsoft 365 to ensure we are making best use of technology
- ensure our digital transformation is underpinned by robust governance and security processes

Business intelligence and data management
Where are we now:

- driving high quality, automated, evidence-based standards for data, to make decisions and manage performance
- data quality and retention managed in key legacy systems
- corporate management of key corporate systems
- use of dashboards to inform local risk and performance management
- linking prevention, protection and response through data management

Where will we be in four years:

- single version of the truth through single source data
- Service-wide use of corporate data via 'Real Time' dashboards
- data management at the forefront of business processes and system development
- data retention protocols established and managed across all systems
- Geographical Information Systems (GIS) at the forefront of intelligence data to help inform business decisions

How will we get there:

- align to the NFCC's data management standard
- migration of corporate systems to hosted environments
- improve systems and availability of real time data to support decision making
- information Asset Owners proactively managing data quality and governance

ICT resilience
Where are we now:

- secure infrastructure and advanced technology, that raises the efficiency and effectiveness of our operational response
- highly resilient, geographically separated data centres, virtual server farms with high-speed links and fallback facilities
- proactive and reactive in-house teams continually maintaining and developing a strong safe infrastructure
- increasingly developed systems and tools to reduce technical administration and align processes for ease of management and increased security of data

Where will we be in four years:

- increased strength in our infrastructure, security and storage to support the development and use of new technologies on the frontline
- increased accessibility protection
- historical products and processes replaced through investment in new, to mitigate our weaknesses and increase efficiency
- accessible information through Apps and use of AI tools for increased business resilience

How will we get there:

- end user devices that match the requirement of the role and are aligned to flexible and sustainable ways of working
- maintain and develop infrastructure that is aligned to the changing technology and security challenges whilst supporting the business
- continued environmental scanning, exposure and development of AI and Microsoft Tools to increase security, and ensure access to information is 'right info, right place, right time'
- replacement of historical products to strengthen our infrastructure and create more efficient joined up environments
- continued server rationalisation into virtual and Cloud based environments

Operational communications, incident ground technology, Fire Control and the Networked Fire Services Partnership

Where are we now:

- resilient emergency resource mobilising capability
- resilient connectivity between the Networked Fire Service Partnership (NFSP) control rooms
- risk critical and incident related information provided to crews on the incident ground via our Mobile Data Terminals (MDT) and risk information tablets (RIT)
- all appliances and officers have digital fireground radios and airwave communications
- maintaining involvement in the Emergency Services Network
- reviewing the opportunities for a dynamic coverage tool

Where will we be in four years:

- further strengthened our mobilising capability, providing more resilient bearers and improving station end user interfaces
- improved and extended our connectivity between our NFSP control rooms, to include Kent FRS, and our CAD supplier
- updating to the latest technology for incident ground communications and information sharing
- enhancing our ability to maintain critical communications between the incident ground and the control room
- cognisant of the need to consider ESN with technological advances and procurement of new solutions
- have a state-of-the-art mobilising system providing resilience across the NFSP to support efficient and effective service delivery
- optimising efficiency by using a dynamic coverage tool to inform resource movements

How will we get there:

- replacement of all station-end mobilising equipment, with advanced user interfaces, and extended abilities through the RIT's. Implementation of the crew and officer app based alerting solution
- procurement of a replacement Wireless Access Network (WAN) to connect our 4 NFSP control rooms and compliment the replacement command and control system
- procurement of replacement MDT's, ABD's (Appliance Bridging Device), RIT's and officer sat nav devices
- implementing incident command, fire survival guidance and electronic forms software along with alternative critical communication methods for our incident commanders
- procure a new command and control system for our Fire Control
- continue to identify and invest in new opportunities to utilise digital technology and training