

# Cheshire Constabulary's IT Strategy 2022-2025



**Cheshire  
Constabulary**



**Police & Crime  
Commissioner  
for Cheshire**



# Foreword

We welcome the development of the IT Strategy which over the next decade will see police technology develop to service the needs of the public of Cheshire and appropriately support the officers and staff of the constabulary.

The IT Strategy sets out how the Commissioner and the Chief Constable will work to ensure Cheshire has fit for purpose and innovative technology which is required to deliver effective operational policing, are connected to communities and which house support functions suitable to serve the public. That they are provided in a way to support policing and enhance community engagement.

It aims to deliver technology which will be more efficient and of lower cost to run, which is flexible enough to respond to the developing service requirements of the local community and to contribute to increasing public confidence in policing. It will allow the Constabulary to maintain and improve high quality services, improve effectiveness, ensure good value for money and an efficient use of resources. It demonstrates the constabulary's commitment to the new digital ambition for UK policing through the National Policing Digital Strategy 2030, and utilising cloud technology to contribute to the constabulary's Environmental Strategy 2021 – 2031.

The strategy underpins the commitments we have laid out within the Police and Crime Plan and the constabulary's policing strategy.

# Introduction

The Digital landscape is the fastest growing area within UK Policing and making our digital services accessible to the public is critical for the long-term stability of public confidence within Policing. New technologies can provide significant societal and policing benefits.

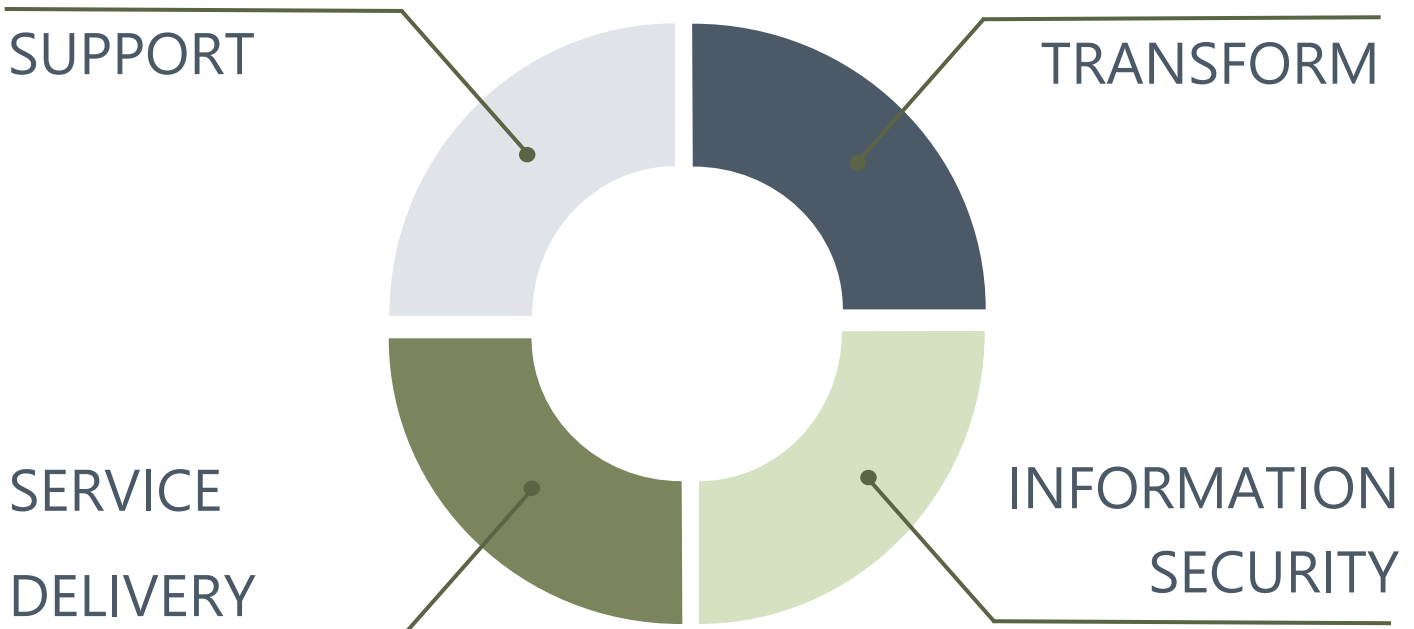
Our aim is to enable and support new ways of working through the introduction of new capabilities, which will drive even greater efficiencies in our services. Cheshire Constabulary puts digital at the heart of its IT Strategy and this document will aim to underpin the force's digital ambition whilst utilising the Raising the Bar performance framework. A key strategic aim is to consolidate on the new technology being introduced and maximise its potential wherever possible.

IT Services are committed to ensuring all of our people have the technology they need to do their jobs well. We will continue to deliver modern technology to our customers and make sure the right equipment is in the right place to suit operational requirements.

The NPCC vision for 2025 and the National Policing Digital Strategy 2020-2030 encompasses all that we aim to deliver, and the Force has already achieved so much toward those visions. The introduction of 2000 tablets to front line officers, 1,500 laptops and 1500 phones have supported the Forces' approach to both agile and mobile working with 82% of staff/officers being agile enabled. The introduction of the first multi-platform deployment and contact system Saab Safe offering a fully integrated solution for operational and public communications.

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

# Key Principles



To deliver our strategy, we will be working on 4 key principles, Support, Transform, Service Delivery and Information Security.

These principles will link directly to the Force Digital Strategy, aligning with the force business requirements. IT will remain business focussed and not simply led by technology.

# Support

One of the key parts of the IT Strategy is to support our frontline and police staff to help deliver the best service to our public. To deliver that, it is essential that we give our staff the right tools to deliver this service effectively and efficiently. It is also important that we give IT support and customer services staff training and information on new technology so that we can provide effective solutions to the force's 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.

We want to attract, develop, and maximise retention, engagement, and productivity of a high-calibre IT professional workforce. This will be a particular focus and we will work with our HR colleagues to provide innovative ways of recruiting and retaining staff.

## **INFORMATION SECURITY AND DATA PROTECTION RISKS ARISING FROM TECHNOLOGY**

As well as developing guidance to support the technology priority areas, we will update our existing technology guidance to reflect the requirements of the new provisions in legislation. We will promote the use of secure by design principles and demonstrate how these contribute to good information security and data protection.

We will deliver a continuous programme of security awareness training to all staff to raise their understanding of threats to them and the organisation, plus how to stop successful attacks that will put the information we hold at risk.

## **OUTCOME**

- The IT Services department staff will be knowledgeable and skilled professionals in both the technical aspects of IT Support and developments but also the information security elements which in turn, will lead to a better supported force.

# Transform

We will make our force fit for the future by introducing new and innovative technology to support officers and staff deliver the best service to our communities. This transformation will also support the NPCC vision for 2025 and the National Policing Digital Strategy 2020-2030

## 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. The Frontline Digital Mobility plan will see the creation and deployment of smartphone applications allowing more operational functions to be carried out in the field. This will enhance the capability of officers on the frontline and drive further operational efficiencies and may see a shift in form factor from traditional tablet to phone

## INTEROPERABLE TECHNOLOGY

Develop interoperable technologies that enable detection of and resilience against threats. The Force is furthering its investment in wireless networks to improve its mobile and agile deployment, achieve and maintain interoperable communications capabilities around the Force and beyond. The Force is working collaboratively with Cheshire West and Chester, and Cheshire East on the 2nd generation 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, whilst working with our partners.

## DIGITAL COLLABORATION

The Force will continue to grow its information sharing capacity by adopting a collaborative approach, utilising shared technology platforms. Building on the deployment of Microsoft 365, we will enhance digital collaboration with our partners through our M365 Transformation workstream. There are significant opportunities for saving effort through improved data handoffs between internal and external parties e.g. MARAC meetings and the ability to share information with other Forces with many of the traditional blockers removed.

## 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 AND STRATEGIC PLANNING

Creating a customer service model to improve delivery of high-quality IT services, including transparent expenditures and Priority based budgeting costs while advancing the adoption of scalable, flexible, cost-effective, accessible services through enterprise and brokered service offerings. Budget pressures will also necessitate improved longer-term financial planning

## MOVING TO THE CLOUD

Continue our success of moving the organisation into the next generation of Enterprise Cloud Computing that facilitate timely provisioning and delivery of services.

## DEMAND MANAGEMENT

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 demand in order to optimise Service Delivery.

## OUTCOME

To deliver the above we will;

- Provide an IT service in accordance with ITIL principles
- Support the transition from traditional service provider models to 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

# Information 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 so that inappropriate audiences (threat actors) do not have unauthorised access. We want to reduce the impact from security incidents and data breaches that have the potential to cause an operational impact and put the public's information at risk.

## **SECURE-BY-DESIGN – ENSURING NEW SYSTEMS MEET BEST PRACTICE**

All technology and systems introduced to the Force should be done in a consistent manner. We will follow National Cyber Security Centre (NCSC) best practice and established NIST/ISO 27001 control frameworks. All systems will be risk assessed with Information Asset Owners assigned who are responsible for the data. A cloud first approach will be followed, whilst still adhering to secure design principles.

## **ENHANCED PROTECTIVE MONITORING**

We will move our protective monitoring capability to the Police National Management Centre ensuring 24x7 coverage, further enhancing protection in this area, sharing threat information with the rest of the Police Service.

## **CONTINUOUS SECURITY IMPROVEMENT**

We will use CHECK based IT Health Checks and pro-active Vulnerability Management to improve our security posture, whilst driving improvements through the use of new toolsets as they become available. Security products will be reviewed on an on-going basis to ensure they are in-line with our defence-in-depth approach.

## **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 from across Policing to ensure common practices are adopted and maintained

# Supporting the Forces Digital Ambition

As an IT department, we will ensure that our own strategy supports the force's digital ambitions and is business and operationally focused. We will link to the digital strategy and providing the resource and support to help deliver other projects within the Force's digital portfolio.

We will:

- Develop mobile applications for the frontline. The Frontline Digital Mobility roadmap will see the creation and deployment of smartphone applications allowing more operational functions to be carried out in the field. This will enhance the capability of officers on the frontline and drive further operational efficiencies.
- Assess and prepare the organisation for the National Enabling Programme which will see the introduction of Microsoft 365.
- Support digital contact initiatives such as live video streaming.
- Implement new change initiatives within existing technologies to solve organisational challenges. A development roadmap has been developed for SAAB, which will see a series of new capabilities introduced into the system.
- Drive forward innovation capabilities such as Robotic process automation. We will automate routine processes to accelerate their execution, but also to increase the proportion of personnel time that is spent on value-add and priority tasks rather than on basic repeatable actions.
- Increase digital collaboration with partners through implementation of new capabilities, such as Digital Evidence Management and our 365 Transformation workstream.

# Raising the Bar

IT operates a mature Performance Management framework. To support the Force's Raising the Bar Performance Framework, we will continue to focus on improving service delivery to our customers and the development of our staff.

IT Surgeries have been further embedded to allow us to work more closely with Frontline officers & staff to get a better understanding of their IT requirements. These surgeries help us to provide a more responsive support to the Frontline. We will continue to resource this initiative, providing opportunity for team members across the department to support these events.

We aim to support team members looking for development, including undertaking short attachments into other teams in the department.

We continue to maintain the Customer Service Excellence (CSE) accreditation which provides an external benchmark of our service to customers and allows us to use that benchmark to further improve service.

## Customer Service Excellence (CSE) - What is it?

'Customer Service Excellence aims to bring professional, high-level customer service concepts into common currency by offering a unique improvement tool to help those delivering services put their customers at the core of what they do'

The CSE Quality Mark is regulated by the United Kingdom Accreditation Service (UKAS)

The standard covers the following areas:

- Customer Insight
- The Culture of the Organisation
- Information and Access
- Delivery
- Timeliness and Quality of Service

We annually review our Customer Service Excellence accreditation in October 21 and to maintain this standard we will need to continually improve year on year.

## Contact

**Email:** [public.contact@cheshire.police.uk](mailto:public.contact@cheshire.police.uk)

**Website:** [www.cheshire.police.uk](http://www.cheshire.police.uk)

**Twitter:** [@cheshirepolice](https://twitter.com/cheshirepolice)

**Facebook:** Cheshire Police

**Address:** Cheshire Constabulary Headquarters  
Clemonds Hey  
Oakmere Road  
Winsford  
CW7 2UA

**Telephone:** 101

