Information and Communications Technology Strategy

2018 – 2025

Date	19 November 2018
Version	0.2
Author	Superintendent Edward Newton
Owner	Assistant Chief Officer Ian Cosh

Contents

1. Summary

Lancashire Constabulary is becoming ever more reliant on technology to achieve its purpose and therefore, our ICT function's core responsibility must be to deliver fit for purpose technology (systems and infrastructure) which improve performance or reduce constraints, whilst ensuring that the services supplied have sufficient capacity, availability, security and continuity assurance.

This document seeks to describe our ICT strategy for the period 2018 – 2025. In doing so it will define how ICT will support and enable our Constabulary Purpose which is *'To keep people safe and feeling safe and when you need us we can be trusted to consistently deliver a competent and compassionate service 24/7'.*

This strategy will be supported by detailed implementation plans for each technical work stream. It is not the purpose of this plan to list all of our activity but to set out our priorities, principles and approach to measuring success.

This ICT strategy will seek to support Lancashire's Police and Crime Plan (2018 - 2021) in which our Police and Crime Commissioner has set four strategic priorities, which are:

- Protecting Local Policing
- Tackling Crime and Reoffending
- Supporting Vulnerable people and victims
- Developing safe and confident communities

Our future investments in technology must act as an enabler to our capability to address and achieve these priorities. Our role as a department is not only to support but also to influence and help shape the future operating model of the Constabulary.

The 2025 NPCC and APCC* Policing Vision states, *"The increasing availability of information and new technologies offers us huge potential to improve how we protect the public. It sets new expectations about the services we provide; how they are accessed and our levels of transparency. Digitisation also offers significant potential to accelerate business processes, manage risk more effectively and revolutionise the criminal justice process".* This statement underlines the criticality of intelligent and considered investment; using the resources available to procure the right technology to meet both current and future policing needs.

*(National Police Chiefs Council and Association of Police & Crime Commissioners)

2. Context

Building on positive foundations

In 2014, Lancashire Constabulary published a four-year ICT strategy which defined five strategic priorities. They were:

1. Continued investment and focus on ensuring the Constabulary's core IT infrastructure / IT applications are fit for purpose from an availability, capability and security perspective
2. To deliver solutions which meet the national Criminal Justice 2016, digitisation requirement.
3. To deliver a capability to facilitate meaningful digital engagement by the public via a range of digital channels.
4. Further improvements in the capability and capacity for mobile / agile working by Constabulary staff.
5. Increased investment in the capability the Constabulary has to effectively share its data and intelligence with partners – both police and other agencies - to reduce demand, risk and vulnerability.

In October 2017, an independent review of progress against this strategy by the Police ICT Company was commissioned by Lancashire's PCC. This review found that *"overall, the force has made significant progress in implementing the objectives of its ICT strategy".* However, keeping pace with the rapidly developing technology sector represents an ever-greater challenge and the Constabulary needs to be able to adapt to changes more dynamically in future. Therefore this new strategy recognises the progress made during the previous four years but focuses on the challenges and opportunities of providing ICT in the policing sector.

A systematic approach

The Constabulary recognises that it needs to take a comprehensive approach to understanding its current technological capabilities and gaps. This encompasses both the wider digital strategy and this complementary ICT strategy, which is focused on the ability of ICT to support digital transformation.

We have engaged with the work undertaken by the 'Crystallise' project supported by the police innovation fund and as a result have published (August 2018) our first three year Digital Strategy using the Crystallise model, a methodology which helps to define our digital capacity and capability. While this covers most aspects of policing, this Digital Strategy will focus primarily on four broad areas:

- Developing our services to the public with the intention of addressing the public's diverse needs and improving public safety
- Developing our workforce capabilities ensuring that our people make the best use of digitally enabled capabilities
- Embracing innovation and collaboration opportunities by capitalising on new technologies that can transform how we work and achieve our Purpose
- Ensuring that there is clear and purposeful leadership and ownership of delivering our digital vision

Security and data protection

Each year the threat of unauthorised access to our systems and information grows and those responsible for these attacks are becoming more sophisticated. The profile of those committing cyber-crime is also diversifying and their motivations can be varied and known to include state sponsored, terrorist, organised crime and commercial advantage. We must continually develop our security measures as the threat changes and ensure that we undertake regular independent checks of our systems and use only supported and up to date applications and hardware.

The new General Data Protection Regulation (GDPR) 2018, *'needs to be at the forefront of policing where the future of personal data protection is concerned'* (Chaucer, 2017). We will therefore need to ensure that those systems that we acquire and support are capable of managing information in full compliance with GDPR. This consideration will be at the forefront of any future application procurement and we will need to work with incumbent suppliers to ensure that our legacy systems become compliant.

Linking to the national picture

The Constabulary is committed to looking beyond its own geographical borders and actively engaging with national transformation programmes. There are currently seventeen national police technology programmes that will provide a range of benefits, for example providing a National ANPR Service (NAS), a single replacement for the current PNC and PND systems (NLEDS) and a replacement for the Airwave network (ESN). While each of these programmes presents the potential for service improvements, they will require local investment in time and resources during transition and need to be factored in to our annual programme plans alongside other local technology initiatives. This means that our own ICT strategy must be sufficiently flexible to adapt to changes in schedule and scope for national programmes. It will also be critical that these national programmes are recognised not just as

technology improvements, but rather as opportunities for transforming how we deliver our core business.

3. Strategic Priorities

Five strategic priorities will underpin our overarching vision 'to provide technology solutions as enablers to our organisational success'. This vision is specifically designed to support our Core Services which are Contact & Response, Local Policing and Serious Crime & Investigation. Our ICT priorities are to:

1. Support the Constabulary Digital Strategy by designing and implementing solutions which enable us to be outstanding in our use of digital technology.

2. Develop and procure systems that can demonstrably, and preferably measurably, improve the effectiveness of our workforce. This includes a sustained focus on mobile and agile working and acquiring technology that is scalable to accommodate growth in demand.

3. Provide services that consider likely future as well as current needs by effectively horizon scanning emerging technologies, understanding our workforces changing needs and making the best investments with available resources. Whilst we will be innovative, any new schemes, where possible, will be tested to ensure they have delivered value for money and benefits elsewhere before they are formally commissioned.

4. Work with public sector partners to develop technical solutions that will improve our ability to share digital data in order to facilitate collaboration, which will in turn enhance our public value and increase public safety.

5. Provide services and technology that are as future-proofed as possible. Those services must have sufficient capacity, availability, security and continuity assurance; not just at the point of commissioning but with the capability to absorb growth in demand.

4. Our Principles

In order to deliver against our strategic priorities we require clearly defined principles. Principles are general rules and guidelines that inform and support the way in which an organisation or function sets about fulfilling its mission. Our principles take cognisance of the 'National ICT Strategic Principles' (NPTC Strategic Working Group, 2017) and are clustered into five themes which relate specifically to the function of ICT and are :

a. People
b. Business
c. Technology
d. Data
e. Applications

a. People Principles

Leadership

To achieve our strategic priorities we will need to provide highly effective leadership at all levels within our ICT department. Our leadership will be visible, transparent and supportive. We will give our people the right tools and skills to do the job. To achieve this we will provide support and guidance, ensuring that we emphasise our operational aims and objectives so that our people know how to prioritise and what is expected of them. We will actively develop the capabilities of our current and future leaders through formal training, coaching and mentoring.

Communications

Effective communications within the ICT department and with our internal and external stakeholders will be critical. We will communicate face to face wherever possible and when not, by a range of methods to ensure the most effective outcome. We will welcome the views, suggestions and ideas of our people and be open to challenge. We will promote an ethos of supporting and enabling the wider business to be effective by working in partnership with the business and by working together to ensure technology meets the whole organisation's needs.

Developing a high calibre work force

We will work hard to retain a high calibre workforce during a period of public sector pay restraint, by investing in the development of our people. We will also use apprenticeship schemes and internships to inject new knowledge and skills and in doing so develop our future workforce.

We will provide high quality learning opportunities both through commercial suppliers and through our relationships with Lancashire's colleges and universities. We will make sure that our people acquire the qualifications that allow them to keep us at the cutting edge of technology developments.

b. Business Principles

Maximising public value

Maximising public value will be at the heart of our decision making about how we use our resources. The ICT Programme Board will provide governance and direction to ensure that we focus clearly on supplying services that support the Police and Crime Plan and our organisational Purpose.

Cloud computing has evolved rapidly over the last few years; so much so that the amount of new choice and capabilities it offers mean it is fast becoming the industry standard - completely transforming the way that IT services are delivered and consumed. Cloud solutions may allow us to reduce our own hosted ICT infrastructure and in doing so make savings however we must also consider that Cloud solutions are typically offered on a subscription model and so our capital requirements may reduce but our revenue spending will grow.

Business continuity

As technology solutions become more pervasive, we become more dependent on them; therefore, we will consider the reliability of our core systems throughout their design and use. We will as far as possible provide our users with the capability to continue their business functions regardless of external events. Hardware failure, natural disasters, and data corruption should not be allowed to disrupt or stop organisational activities. Recoverability, redundancy, and maintainability will be addressed at the time of design. We will be mindful that business continuity is costly and therefore focus on using our resources to prioritise core systems.

Information Management

Information management is every member of the organisation's responsibility. ICT are our custodians of information and manage the way it which it is stored but the asset management of that data will be the responsibility of thematic business leads.

Without robust information assurance governance and processes, there is a significant risk of compromise, potentially leading to the facilitation of crime, public safety issues, hindrance to investigations, financial loss, damage to our organisational reputation and, consequently, a reduction in confidence from the public and partners. Technology initiatives will not begin until they are examined for compliance with our organisational requirements, national guidelines and legislation.

Common Use Applications

We currently (2018) support 390 applications and this number could grow as we become more dependent on technology as an organisation. This creates an increasingly complex challenge of managing those applications and financial burden relating to the consequential licence costs. We will

therefore avoid acquiring or developing similar or duplicative applications which are only used by a subset of users.

Regional & National Delivery in mind

Technology solutions should be designed with the long term aspiration of delivery on a national policing footprint although in the interim we should aspire to regional collaboration as a first step. New technology initiatives must provide interface capabilities (APIs) and interoperability with the purpose of providing an ability to share and analyse information. A technology solution's capability to become part of a regional or national solution should be considered during the design phase of each project.

National Police and Criminal Justice initiatives

There are currently seventeen national transformation programmes which will provide wide ranging technological solutions to UK policing. To ensure we capitalise on the business benefits of these initiatives we will work in partnership with the various programmes to ensure that this Constabulary embraces the opportunities presented, by transforming how we do our business in ways that emerging technologies support.

Customer first approach

Effective technology enables a workforce whilst poor technology can be at best a hindrance and at worst catastrophic to any organisations ability to function. We will provide high levels of customer service to our workforce and partners. We will achieve this by providing an efficient and effective method to contact our ICT department and to log and record requests and incidents. We will develop our self-service offer to users to standardise our services and reduce the time it takes to resolve issues.

Partnering with Excellence

Making the best use of technology and identifying emerging opportunities requires us to partner with excellence both in the private and public sector. We will continue to use the methodology of working with a strategic technology business partner and seek out proven experts in the commercial technology sector for advice and support in specialist areas of our ICT business.

We will be an intelligent consumer of ICT by designing detailed statements of requirements which are outcome focused and by retaining a comprehensive view of the market. Our procurement will be transparent and compliant with regulations and we will undertake careful due diligence before investing.

Information Technology Infrastructure Library (ITIL) Framework approach

The ITIL framework is recognised as the IT industry standard source of best practice in service management. We will embrace the ITIL framework to define how we deliver our services through the lifecycle of Strategy, Design, Transition, Operation and Continual Service Improvement. To achieve this we will train our people and qualify them in ITIL practice.

Responsive Change Management

Changes to the organisational information and technology environment will be implemented in a timely manner. If people are to be expected to work within the organisational information environment, that information environment must be responsive to their needs. We will develop processes for managing and implementing change that do not create delays. This approach recognises the necessity for technical, user and information security due diligence which will be balanced with a dynamic change philosophy.

c. Technology Principles

Consider Cloud First

Services such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) will be considered for cloud hosting above local on premise hosting where applicable to ensure services can develop and evolve. It will not always be in the organisations best interests to select cloud solutions and each requirement will be carefully evaluated. This approach will allow for the delivery of solutions that can be scaled and to facilitate future collaboration where appropriate. When cloud solutions are selected, those hosted services will be designed to fully utilise the capabilities of the platform, including scaling and authentication. To achieve a consistent approach we will develop a supporting Cloud Strategy which underpins this core document and allows us to weigh the benefits of digital information management options.

Control Technical Diversity

When introducing new technology to manage information, it should be considered as a replacement for an existing environment rather than additive if possible. Failure to decommission legacy systems leads to unnecessary infrastructure, licensing and support costs and is inefficient.

Interoperability

Software and hardware will conform to defined standards that promote interoperability for data, applications, and technology. Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing ICT investments. Standards for

interoperability additionally help ensure support from multiple vendors for their products, and facilitate supply chain integration. Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution.

d. Data Principals

Data as an Asset

Data is an asset that has value to our organisation and must be managed accordingly. This is vital for maintaining public confidence and for the efficient, effective, safe and secure conduct of operations and services. Without robust information assurance governance and processes, there is a significant risk of compromise, potentially leading to the facilitation of crime, public safety issues, hindrance to investigations, financial loss, damage to organisational reputation and a reduction in the confidence of the public and partners. Information Asset Owners (IAO) will be given the support and authority to manage the data for which they are accountable in line with MOPI and GDPR.

Information Asset Owner

Each data asset will have an Information Asset Owner accountable for it. As the degree of data sharing grows and business units rely upon common information, it is essential that only the Information Asset Owner makes decisions about the content of data. Since data can lose its integrity when it is entered multiple times, the Information Asset Owner will have governance responsibility for ensuring the integrity and accuracy of that data.

Data is shared

We will provide timely access to accurate data. This is essential to improving the quality and efficiency of decision-making. Shared data will result in improved intelligence and decision making since we will rely on fewer sources of more accurate and timely managed data for all of our decision-making.

Data is Accessible

Wide access to data leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery. We will facilitate legitimate access to information by the widest range of users with the purpose of saving our workforce's time and so that the consistency of data is improved.

Data Security

Our data must be protected from unauthorised use and disclosure in line with the Government Security Classification model. Sharing of information and the release of information via relevant legislation will

be balanced against the need to restrict the availability of classified, proprietary, and sensitive information.

We will continue to embrace a 'strength in depth' approach in respect of the security of our systems and information by constantly developing protection from cyber-crime, and other modern day threats which is multi layered and predicated on the principal of utilising a range of tools and technology to prevent unauthorised access but in the case of a breach, limit that access and deny it as quickly as possible.

e. Application Principals

Ease of Use

We will develop and procure applications that are intuitive and easy to use and by doing so ensure most of the knowledge required to operate one system will be similar to others. We do recognise that this approach requires the availability of commercial application solutions that fulfil this requirement but by doing so, training will be kept to a minimum and the risk of using a system improperly will be reduced.

Single Authentication Model

Where feasible we will ensure that user authentications are delivered from a single central user directory. This will simplify the user experience, while improving security and not require any repetition of credentials to be provided by the user unless unavoidable.

For cloud or hosted solutions, the authentication platform should be federated to our force directory allowing administration to occur locally using the existing tools and processes.

When the National Enabling Programme delivers an IAM solution our cloud and hosted applications will utilise this platform to perform user authentication.

5. Governance

Delivery of effective and efficient ICT services is essential to this Constabulary's capability to perform its core Purpose of protecting people and our annual IT investment represents in excess of 5.5% of our combined capital and revenue budget and for these reasons, clear governance of our ICT Strategy and approach are required.

Governance will be achieved by means of an ICT Programme Board which will be chaired by the Director of Resources / Senior Information Risk Owner and its membership will be made up of key strategic stakeholders. The Head of ICT will also report directly to the holder of this post.

This Board will be charged with deciding which ICT projects and activities are progressed and their order of prioritisation. The Board will use a structured and transparent decision making methodology based on a 'Project Risk and Complexity' matrix to decide where investments in resources should be placed.

An annual Capital Plan Funding Bid will be submitted to the OPCC for approval by the Police and Crime Commissioner which will provide a detailed description of projected spending requirements over a five year forecast.

The Head of ICT will also report on a monthly basis to the Strategic Management Board chaired by the Chief Constable and be a member of the Executive Leadership Team. Through these forums clear direction and consultation with Chief Officers and heads of other business areas will be achieved.

6. Measuring Success

Delivering effective ICT is based on the four essential cornerstones of capacity, availability, security and continuity. These are quantitative and easy to measure by reference to diagnostics and system management data. We will use data analytics to combine this information into a dashboard to be used as a key performance management tool.

We will measure to what extent we deliver fit for purpose technology (systems and infrastructure) which improves performances or reduce constraints by listening to our internal and external stakeholders. We will be held to account by those who we supply services to.

Through membership of the National Police Technology Council we will compare our progress with other UK police forces and use this as a benchmark of our success in maintaining a position at the cutting edge of technology in the policing sector.

We will conduct independent and anonymised staff surveys to assess the wellbeing of our ICT people and use our HR system reporting tools to measure the overall health of our workforce.

We will measure value for money independently through reference to the HMICFRS 'most similar group' (MSG) forces comparison reviews. This Constabulary currently sits within the lower quartile of the MSG and we will aim to remain there.