

<b>Meeting</b>	<b>Authority Meeting</b>
<b>Date</b>	<b>30 September 2020</b>
<b>Location</b>	<b>Video Conference</b>
<b>Title of Paper</b>	<b>Police Scotland Cyber Strategy</b>
<b>Presented By</b>	<b>DCC Malcolm Graham, Crime and Operations</b>
<b>Recommendation to Members</b>	<b>For approval</b>
<b>Appendix Attached</b>	<b>Yes</b>  <b>Appendix A – Cyber Strategy</b>

**PURPOSE**

The purpose of this paper is to update members on the development and implementation of Police Scotland's Cyber Strategy, *Keeping People Safe in the Digital World*.

This is an enabler strategy underpinning and supporting the Joint Strategy for Policing (2020), *Policing for a Safe, Protected and Resilient Scotland*. The strategy sets out Police Scotland's approach to contribute effectively to the following strategic outcome and objective:

Strategic outcome 1: Threats to public safety and wellbeing are resolved by a proactive and responsive police service

Objective 1: Keeping People safe in the physical and digital world

The SPA Board is asked to approve the strategic direction set out in the Cyber Strategy and to endorse the approach to investment & financial planning to support successful implementation.

## 1. BACKGROUND

- 1.1 In *Policing for a safe, protected and resilient Scotland*, we committed to the development of a pioneering cyber strategy for Police Scotland with the aim of enabling us to transform Police Scotland's capacity and capability to respond to threats and establish various ways to prevent, disrupt and respond to the ever more inventive and complex use of digital tools and new tactics, often originating from beyond our borders.
- 1.2 Cyber enabled and cyber dependent crime has been increasing for a considerable period of time and this has escalated further during the COVID-19 pandemic. This is an area of increasing risk and Police Scotland must ensure that our policing model can respond effectively.
- 1.3 Good progress has been made to date, including the roll out of digital triage and mobile devices and addressing legacy issues to streamline our core operational systems through the digitally enabled policing programme.
- 1.4 Police Scotland's critical role during the COVID-19 pandemic has been recognised, most recently in the Programme for Government 2020-21. This sets out a Scottish Government priority to ensure Scotland is safely and securely able to develop smart digital solutions to meet the needs of the immediate and long term economic future. Both the UK and Scottish Governments are refreshing their own Cyber Resilience Strategies in the next 12 months (subject to COVID-19) and close working has been in place to share insights and align strategic thinking, as appropriate.
- 1.5 The Police Scotland Cyber Strategy sets out our future aspirations and strategic direction to ensure that Police Scotland can continue to keep Scotland's people, communities and assets safe in both the physical and digital world.

### **Development of the Cyber Strategy**

- 1.6 The Cyber strategy has been designed and developed with the support of a strategic oversight group Chaired by DCC Graham. A full range of strategic assessment, research and a landscape review was undertaken along with an extensive range of internal and external stakeholder engagement. The views of the public and communities were sought as part of the consultation on the joint

strategy and have been considered as the cyber strategy has been developed.

- 1.7 The Scottish Police Authority has been engaged, supportive and provided helpful challenge throughout the design and development of the strategy. This included feedback as members of the Cyber Resilience and Digital Capability Board and a workshop session with all Board Members to consider the proposed approach, challenge the strategic direction and consider in more depth areas such as investment, financial planning and the implications of the cyber strategy for the first Police Scotland Strategic Workforce Plan. This input and feedback has been included in the final strategy.

### **Objectives and enablers**

- 1.8 The cyber strategy focuses on the following four objectives to address a range of key internal and external areas where the service needs to design, develop and implement new approaches for the future.

**Police Scotland resilience** Ensuring that Police Scotland is resilient and able to respond to shifting threats

**Public health, prevention and partnership** Working holistically and sustainably to prevent cybercrime by developing a public health approach and working effectively with partners

**Investigation of criminality** Making Scotland a challenging place for cyber criminals to operate by increasing our visibility in the physical and virtual world

**Protecting and safeguarding** Ensuring that our focus on protecting and safeguarding those at most risk of harm continues to be at the forefront of all we do

- 1.9 Due to the critical, broad and cross cutting areas of policing within the strategy and to support implementation and planning, five enablers have been considered to ensure that Police Scotland has a holistic approach to successfully achieve our objectives.

**Respecting rights** Continuing to build trust and confidence by involving the public, communities and businesses as we design our approach to cybercrime

<b>Capacity and capability</b>	Working to adjust our policing model to meet the needs of the public, communities and businesses of Scotland
<b>Infrastructure</b>	Focus on transformation and investment in our infrastructure to enable Police Scotland to be an efficient and effective policing service
<b>Data driven innovation</b>	Promote and develop our relationships and culture to drive innovative solutions that enable our cyber strategy
<b>Investment</b>	Using our existing resources with targeted spend to save investment will allow us to achieve our cyber objectives

1.10 Implementation planning for the strategy will involve a comprehensive exercise to understand and set out the baseline for services ahead of further steps to make changes in line with the strategic direction.

1.11 Implementation of the strategy will achieve the following important changes to ensure policing can continue to meet the current levels of risk, threat, harm and increasing demands:

- Increased visibility of policing in both online, and physical spaces that supports our ability to tackle cybercrime proactively.
- Embracing the shift to a new policing model that is equipped to tackle the demands of cybercrime, and safeguard communities.
- By adopting a whole public system approach, we can use our data to identify opportunities to prevent victimisation of at risk individuals.
- Investment in our systems and infrastructure to ensure it is secure by design, and fit for purpose.
- Strategic choices on how we mobilise and deploy resources most effectively.
- Proactive and agile approach to partnerships will support the mutual development of innovative solutions.
- Opportunities will be explored for officers and staff to use their specialist knowledge and experience to develop our capabilities.

- Local policing will be enabled to identify and investigate cybercrime as first responders.

## **2. Next Steps**

- 2.1 An exercise to establish an appropriate baseline will be undertaken alongside the development of an implementation plan to set out the roadmap for the strategy to be implemented, closely aligned to financial and strategic workforce planning underway at present.
- 2.2 Further engagement with the SPA will take place on a regular basis, particularly in relation to areas such as investment, financial and strategic workforce planning to ensure that the agreed direction continues to be fully aligned.

## **3. FINANCIAL IMPLICATIONS**

- 3.1 There are no direct financial implications in this report, however, investment requirements will be set out as part of the financial and change planning processes for 2021 and beyond.

## **4. PERSONNEL IMPLICATIONS**

- 4.1 The personnel implication of this strategy will be set out in more detail within the Strategic Workforce Plan.

## **5. LEGAL IMPLICATIONS**

- 5.1 There are no legal implications associated with this paper

## **6. REPUTATIONAL IMPLICATIONS**

- 6.1 There are reputational implications associated with this paper.
- 6.2 The changes outlined by our ambitions within the Cyber strategy are necessary in order to maintain and build public confidence in our capability to respond to this area of increasing demand.

## **7. SOCIAL IMPLICATIONS**

- 7.1 There are no social implications associated with this paper.

## **8. COMMUNITY IMPACT**

- 8.1 There are no community implications associated with this paper.

## 9. EQUALITIES IMPLICATIONS

- 9.1 There are equality implications associated with this paper. A summary EQHRIA has been completed for this strategy and will be published.

## 10. ENVIRONMENT IMPLICATIONS

- 10.1 There are no environmental implications associated with this paper, however, the implementation plan is likely to identify areas that can support Police Scotland to reduce our overall environmental impacts.

## RECOMMENDATIONS

The SPA Board is asked to approve the strategic direction set out in the Cyber Strategy and to endorse the approach to investment & financial planning to support successful implementation.

# Cyber Strategy 2020

Keeping people safe in the digital world



**POLICE  
SCOTLAND**  
Keeping people safe  
**POILEAS ALBA**

**SCOTTISH POLICE  
AUTHORITY**

# Contents

<b>Foreword</b> .....	<b>3</b>
<b>Executive summary</b> .....	<b>5</b>
<b>Strategy overview</b> .....	<b>9</b>
Purpose of the strategy .....	10
Current state assessment .....	12
<b>The case for change</b> .....	<b>15</b>
<b>Our vision and objectives</b> .....	<b>19</b>
Cyber resilient .....	21
Cyber investigation .....	33
<b>Our enablers</b> .....	<b>47</b>
Respecting rights.....	47
Infrastructure.....	48
Capacity and capability .....	49
Data driven innovation .....	52
Investment.....	53
<b>Strategic alignment and performance</b> .....	<b>55</b>
<b>Governance</b> .....	<b>58</b>



# Foreword



In Policing for a Safe, Protected and Resilient Scotland, our Joint Strategy for Policing (2020), we highlighted the need to keep people safe in both the physical and digital world.

The pace of technological change and digital connectivity continues to accelerate and grow, now reaching into almost every part of daily life. Whether as active participants using multiple devices, programmes and platforms in our work and home life, or as customers, clients or contacts of organisations and companies, we have never been more connected.

Enhanced connectivity and instantaneous communication, while offering great opportunities, also presents risks and new vulnerabilities

for individuals, communities and organisations. This is a global challenge that reaches beyond our own borders.

As communities change we are adapting how we are visible and accessible to them, operating across both physical and virtual environments. There has been a significant rise in digitally enabled and dependent crime, increasing the scale of additional demands faced by policing. Police Scotland will increasingly extend its presence into the digital world and as a consequence, we will ensure that our services are appropriately resourced to meet the needs of our communities.

This strategy sets out how Police Scotland will take a proactive approach to respond to cyber demand, ensuring that we are future focused and able to adapt our policing model to suit the needs of the communities we serve.

We will adapt our service to respond to and pre-empt changes in the volume, type and complexity of demand we face on a day-to-day basis.

At an ever-increasing pace, criminals and their networks are using new technologies and connectivity to exploit citizens, businesses and institutions. At the same time, traditional crimes overwhelmingly now involve a digital element and require Police Scotland to gather, sort, analyse and present significant volumes of digital evidence.

As we continue to live through a global pandemic that has prompted even greater reliance on digital technologies in our work and home life, increased vulnerability has also arisen. Police Scotland has a vital role to play to provide advice and reassurance while vigorously pursuing those who would cause harm to our people, communities and businesses. The cyber capability and capacity of policing in Scotland has been undermined by historic underfunding over many years. Wherever possible we will adapt our existing services and funding to a model and approach that will meet that challenge, with targeted investment in areas where we need to make the most rapid progress.

The communities we serve will benefit from embedding cyber resilience and investigation into everyday policing. Local policing will play a significant role in the investigation of cyber enabled crime allowing our specialist cyber services to be deployed to maximum benefit.

Developing new and existing partnerships will ensure that we are able to protect the public and businesses, while safeguarding those most vulnerable to cyber threats.

Key partnerships will enable us to develop and incorporate the technology and data we need to prevent and disrupt online criminality in all its forms. New technologies and data sharing provide opportunities and enhance

the effectiveness of policing. We will ensure a strong and consistent ethical oversight that is open to scrutiny and maintains public confidence.

Our approach to policing is built on our shared values of fairness, integrity, respect and supporting and enabling human rights. As we live more of our lives online and we see risk and vulnerability increase, we will seek to strike the right balance between privacy and protection.

As one of the largest organisations in the Scottish public sector we have a responsibility to protect the service we provide from both cyber-attack and systemic vulnerabilities. Policing in Scotland is based on consent and trust, and we must safeguard our own cyber security and resilience in order to exercise our duties to the public.

In order to embed cyber capability and capacity into Police Scotland, we must invest in our people, ensuring that they have the right tools and skills to keep pace with cyber criminality. By developing cyber skills and resilience throughout the organisation we will provide our people with effective training to investigate cyber and online crime, complementing their existing skillset. To make certain we have the right people in the right place, we also need to attract, recruit and retain those with the expertise required.

Police Scotland has a duty to protect all of the people of Scotland in the public, private and virtual space. This strategy will help to ensure that we achieve that core duty.



**Iain Livingstone QPM**  
Chief Constable

# Executive summary



**Malcolm Graham**  
Deputy Chief Constable,  
Crime and Operations

## Introduction

We all recognise the changing world we live in. Successive policing strategies, most recently the Joint Strategy for Policing (2020) agreed with the Scottish Police Authority, Policing for a Safe, Protected and Resilient Scotland, have a clear focus on the need to adapt how we police to keep people safe in the digital world.

Police Scotland is working towards strategic outcomes that describe the impact we want to have for the people of Scotland. Under the outcome 'Threats to public safety and wellbeing are resolved by a proactive

and responsive police service', we have set the objective 'To keep people safe in the physical and digital world'.

In our Joint Strategy we committed to develop a Cyber Strategy for policing that would address how operational policing will meet the challenges we face in an increasingly digitally enabled and online world. Cyber enabled and dependant crime have been increasing for a considerable period of time, which has escalated further during the COVID-19 pandemic. This is an increasing area of risk and requires us to ensure that our policing model can respond effectively.

We have already made good progress including roll-out of digital triage and mobile devices to frontline officers, and addressing historic issues to streamline our core operational systems through our Digitally Enabled Policing programme.

We will continue to protect the rights of the communities we serve and embed our values into everything we do. Fairness, integrity, respect and human rights will continue to be our guiding principles as we aim to improve our cyber capacity and capability.

Police Scotland is a major public sector organisation and our critical role during the COVID-19 pandemic has been recognised. In the 2020/21 Programme for Government, the Scottish Government set out a key priority to ensure Scotland is safely and securely able to develop smart digital solutions to meet the needs of the immediate and long term economic future. Our Strategy sets out our future aspirations and is fully aligned with government policy, setting out a holistic and ambitious approach to how we equip and enable officers and staff across the service to police effectively in all environments, and safeguard our own cyber resilience to allow us to do so.

### **Case for change**

The case for change is driven by a complex set of challenges that modern policing in Scotland is facing, namely:

- Escalating risk of threat and harm
- Changing demands
- Enabling effective policing

### **Escalating risk and harm**

In recent years there has been a steady trend of cyber enabled and cyber dependant crime increasing in Scotland, and the wider UK. As communities increasingly spend more of their time using internet-connected devices and residing in online spaces, exposure to criminal and malicious actors has increased in tandem. Underreporting of cybercrime presents a significant challenge to policing as we know that the data available doesn't clearly represent the true scale of this criminality.

In order to effectively safeguard these spaces we must make our presence more visible online, ensuring education and prevention services are available and accessible to the public.

### **Changing demand**

It is clear that the frontline of policing in Scotland is being blurred by the use of technology to aid, and facilitate crime. These criminal acts are steadily increasing in their frequency and complexity, placing new forms of demand on our resources and personnel. To meet these changing demands we must commit to implementing a new policing model that recognises technology as both a challenge and an enabler for modern policing.

### **Enabling effective policing**

With technology rapidly developing and becoming increasingly accessible to the public, policing and safeguarding in online spaces has never been more important. Undertaking this represents a significant shift in our operational policing model, and will require us to push into uncharted territory for policing in Scotland. In order to navigate this effectively, we must develop clear strategic direction to chart the best way forward, and ensure that we work collaboratively to create approaches supported by our partners and communities.

## Objectives and enablers

The strategy focuses on four objectives:

Police Scotland Resilience	Ensuring that Police Scotland is resilient and able to respond to shifting threats.
Public Health, Prevention and Partnership	Working holistically and sustainably to prevent cybercrime by developing a public health approach and working effectively with partners.
Investigation of Criminality	Making Scotland a challenging place for cyber criminals to operate by increasing our visibility in the physical and virtual world.
Protecting and Safeguarding	Ensuring that our focus on protecting and safeguarding those at most risk of harm continues to be at the forefront of all we do.

Our objectives are supported by five enablers. By bringing these elements together as we progress to implement our strategy, we give ourselves the best opportunity to successfully achieve our objectives:

Respecting Rights	Continuing to build trust and confidence by involving the public, communities and businesses as we design our approach to cybercrime.
Capacity and Capability	Working to adjust our policing model to meet the needs of the public, communities and businesses of Scotland.
Infrastructure	Focus on transformation and investment in our infrastructure to enable Police Scotland to be an efficient and effective policing service.
Data Driven Innovation	Promote and develop our relationships and culture to drive innovative solutions that enable our cyber strategy.
Investment	Using our existing resources with targeted spend to save investment will allow us to achieve our cyber objectives.

## Key changes

### The changes introduced by the strategy will be:

- Increased visibility of policing in both online, and physical spaces that supports our ability to tackle cybercrime proactively.
- Embracing the shift to a new policing model that is equipped to tackle the demands of cybercrime, and safeguard communities.
- By adopting a whole system approach, we can use our data to identify opportunities to prevent victimisation of at risk individuals.
- Investment in our systems and infrastructure to ensure it is secure by design, and fit for purpose.
- Strategic choices on how we mobilise and deploy resources most effectively.
- Proactive and agile approach to partnerships will support the mutual development of innovative solutions.
- Opportunities will be explored for officers and staff to use their specialist knowledge and experience to develop our capabilities.
- Local policing will be enabled to identify and investigate cybercrime as first responders.

## Investment

To deliver this strategy we must invest strategically and significantly. A level of capital and reform funding will be required to make the rapid progress required, and we will target new investment on a 'spend to save' basis, where possible. Together with investment in technology and training, we will also release capacity from our existing officer and staff resources so they can be upskilled and deployed to meet current and future demands.

## Implementation

The implementation programme, setting out how we will deliver and subsequently measure the success of this strategy, is aligned with our other enabler strategies and will feed into our plans, including our strategic workforce plan. Engaging with our people during development and future implementation will be key to successfully delivering this strategy.

## Conclusion

This cyber strategy is ambitious, but delivering on that ambition is critical if we are to keep people safe in the digital world. This strategy has been developed over time to ensure that we have tested our direction against the broader cyber security and policing landscape, industry developments and our own progress in transformation. This strategy is the result of careful consideration ensuring that this redesigned model for policing in Scotland meets the overall needs of the public, communities and business in Scotland into the future.

# Strategy overview

## Our Case for Change

The demands faced in policing are becoming increasingly complex and the resources available to meet these demands continue to be stretched. We need to adapt and change to provide a relevant effective modern policing service, fit for the digital age, which builds and maintains public confidence.



### Outcome

Threats to public safety and wellbeing are resolved by a proactive and responsive police service

### Objectives

- Keep people safe in the physical and digital world
- Design services jointly to tackle complex public safety and wellbeing challenges
- Support policing through proactive prevention

## Police Scotland: Cyber Strategy

*Keeping people safe in the digital world*

### Our strategic objectives

#### Cyber resilient

to capture digital opportunities for keeping people safe and enable Police Scotland, the public and organisations to recognise, resist and respond to cyber incidents effectively

Police Scotland resilience

Prevention & partnership

#### Cyber investigation

to effectively pursue those responsible for cybercrime while protecting and safeguarding victims

Investigation of criminality

Protecting & safeguarding

### Enabled by

Our infrastructure

Respecting rights



Capacity & Capability



Data Driven Innovation



Investment

## **Purpose of the strategy**

Policing for a Safe, Protected and Resilient Scotland, our Joint Strategy for Policing (2020) details our long term strategic direction and sets out the associated outcomes and objectives. Strategic outcome one looks to ensure that threats to public safety and wellbeing are resolved by a proactive and responsive police service. To achieve this, we must work towards our objective; to keep people safe in the physical and digital world.

We have seen rapid technological advances in recent years resulting in easily accessible virtual worlds that underpin, and are entwined with the physical world. This has been accelerated by disruption caused by COVID-19 and the increased reliance on technology, which has placed unprecedented demands upon policing. While these represent significant challenges, they should also be viewed as an opportunity to re-evaluate how we do things.

The purpose of this strategy is to recognise the future demands that will impact on policing in Scotland, and set out how we will anticipate, prepare and respond. This includes ensuring that we have the capacity and capabilities necessary to adapt to that changing environment.

Through exploring these issues comprehensively, we will implement our strategy, and outline our commitments to ensuring we have the necessary skills, partnerships and technology to become a police service that is a centre of excellence in cyber and digital capabilities. This work is fundamental to ensuring that we can continue to successfully investigate cybercrime, support businesses and protect communities.

## **Understanding cyber and threat**

The term 'Cyber' has no universally agreed definition and has become an all-encompassing term for the marriage of technology to other domains. 'Cybercrime', for example, is the involvement of technology in criminal activity, and 'cyber security' is the field of knowledge or practice focused on the protection of information in all its forms from unauthorised disclosure, alteration or denial of access to unauthorised parties.



## Categories of Cybercrime

Cyber dependent	Cyber enabled
The commission or attempted commission of crime in order to compromise a computer device, network or system where the devices are both the tool for committing the crime and the target of the crime. A computer includes a laptop, smart phone, tablet, smart TV or other internet enabled device.	The commission of or the attempted commission of traditional crimes such as theft, extortion, threats etc, using the Internet, or by otherwise accessing a computer, system, device or network.

### Technology in policing

The explosion of new technologies available for use present incredible opportunities for law enforcement agencies, but budget constraints mean many are finding it hard to make the necessary investments in new technologies.

### Technology in criminality

The use of technology to commit or facilitate crime is an everyday reality facing law enforcement agencies worldwide. Organised crime networks in Scotland are using technology to assist with criminal activity. From using their own communication networks, to employing their own technical surveillance counter measures, exploitation of technology to support criminality is now affordable and expected of criminal groups.

## Current state assessment

A recent assessment of Police Scotland's cyber capability by Leonardo indicated areas for improvement and investment to provide effective and efficient services. Areas identified for development include the legacy underfunding of our ICT infrastructure, the increased need for prevention of digitally enabled crime and harm and a need to continue to evolve from the traditional 'physical world only' policing models. However, the assessment also highlighted that Police Scotland has the potential to become a leading force in the UK if it adopts changes in its service management and allocation of resources in regards to cybercrime and digital investigation services.

The demand from cyber enabled crime is increasing and largely reflected in financial and economic crimes, sexual offences and threatening behaviour. These often target the most vulnerable people in our communities.

Currently our limited number of skilled resources can only undertake predominantly reactive investigations into incidents that pose the greatest threat.

In 2018 Police Scotland published an ambitious Digital, Data and ICT (DDICT) strategy that aims to fundamentally change and improve how we invest in technology and its use across the service. The DDICT strategy addresses key issues, and charts a pathway of changes needed to enhance our overall infrastructure, capacity and capability.

## Current capabilities and services

Our Contact, Command and Control division (C3) is most often the first point of contact for people through our telephone, online and British Sign Language channels.

The implementation of the Contact Assessment Model (CAM) has improved the way we triage and respond to contact from the public. This model uses enhanced assessment and decision-making based on threat, risk and harm.

If a relevant crime type is identified this will then, depending on the nature and severity be allocated to local response officers to attend and investigate. In the case of more serious and/or harmful offences, or a crime is in action, it will be allocated directly to specialist officers to investigate and deal with. Using this model, we will be able to engage with victims of cybercrime in the first instance and provide direct support, or access to guidance and resources needed. By developing this capability we can ensure that we provide comprehensive protection to our communities, and enable them to take steps to keep themselves safe.

We have a national approach to cybercrime investigation within Specialist Crime Division (SCD) with Cybercrime Investigations and Digital Forensics providing national coverage and specialist operational support to all divisions across Scotland.

Within the specialist divisions and in the Safer Communities division, there are a number of functions that are responsible for different aspects of cybercrime and work collaboratively to provide a comprehensive service.

Specialist Cyber Teams	
Cyber Harm Prevention Team	Responsible for leading on cybercrime prevention/ internet safety and co-ordinates cybercrime prevention development in partnership with key internal and external partners.
Cybercrime Investigations	Responsible for providing specialist support and undertaking investigations into high-end cyber dependent crimes.
Cybercrime Digital Forensics	Responsible for carrying out examinations and analysis of digital devices/CCTV as well as providing expert advice, specialist recovery services and reports for court.
Cybercrime Policy and Co-ordination	Provides a single point of contact for cybercrime investigations and digital forensics. Responsible for oversight of all related policy and processes.
Intelligence Support	Responsibility for assessment, development and enrichment of intelligence products on behalf of Police Scotland; whilst shaping overt and covert responses to current and emerging threats and risks.

These resources provide specialist advice to officers, staff and our communities on how to prevent, detect and disrupt cyber criminality.

Demand currently outstrips our capacity in this area of business and this situation will worsen if we do not match increasing demands with sufficient resources.

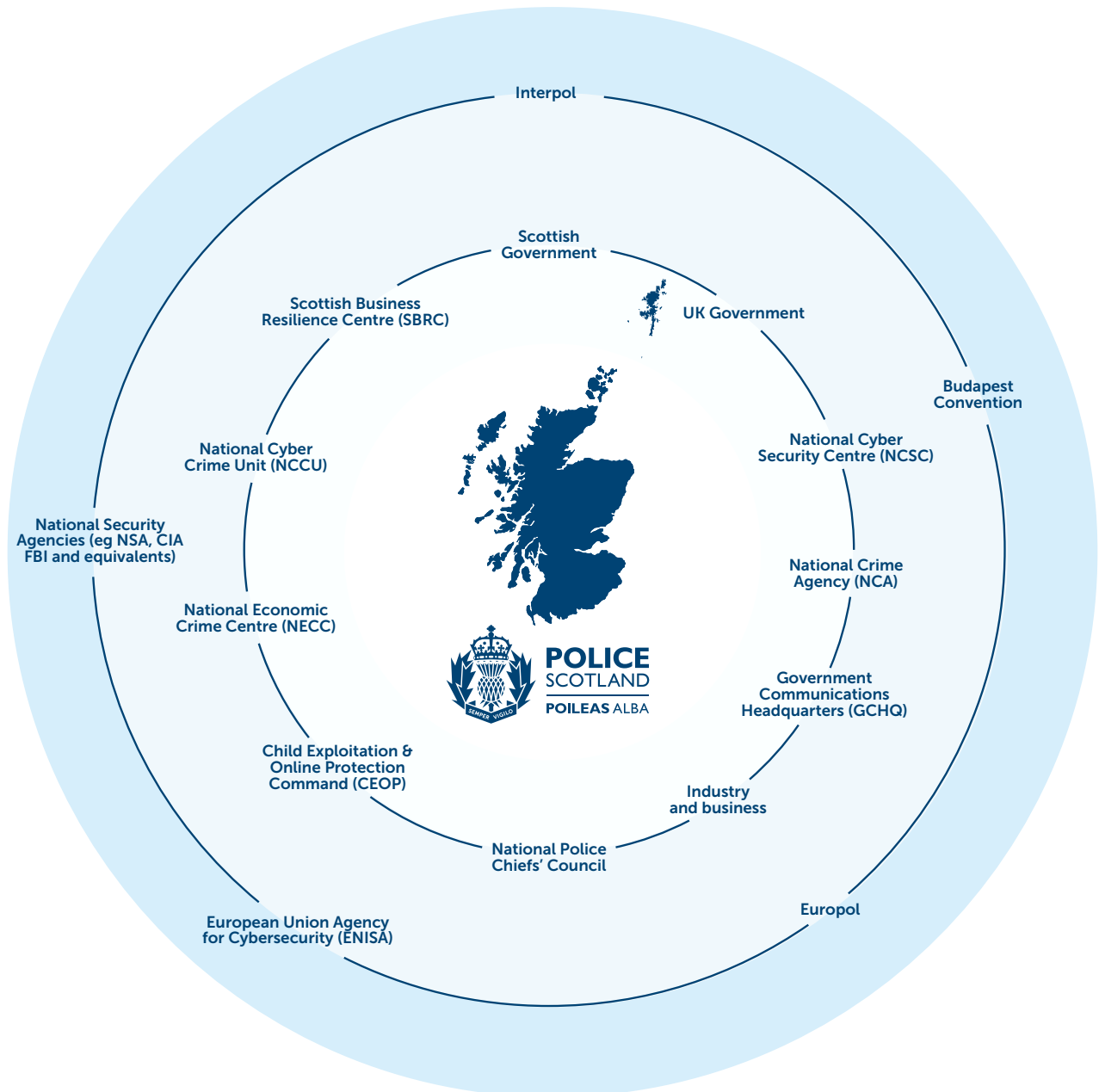
**Ongoing cyber development - Cyber Capabilities Programme**

The Cyber Capabilities Programme (CCP) is a multi-year transformation programme that focusses on building the capacity and capability of our cybercrime investigation and digital forensic services.

The programme aims to review and develop the current service delivery models ensuring cyber dependent and cyber enabled crime is managed effectively and that our people are equipped with the required knowledge, skills and technology to tackle it. CCP aims to support all areas of Policing and has implemented a number of significant changes to date including the cyber hub network, digital triage, cybercrime markers, specialist training and quality assurance. CPP is also leading on the delivery of applications that enable the analysis of vast volumes of data not previously available in Scotland.







## The national cyber landscape

We collaborate with public sector partners to develop a whole public system approach in order to jointly design and tackle complex public safety issues and ethically share data insights. We need to continually review and refine roles and responsibilities with key law enforcement partners for maximum efficiency, effectiveness and best value.



# The case for change

The need for a new approach to cyber is driven both internally and externally.

Our case for change			
	<p><b>Political</b>            Significant political uncertainty with Brexit and potential Scottish independence referendum in the near future.            The implementation of GDPR legislation now guides the way that we use data.            New technologies require us to strike the right balance between privacy and protection.</p>		<p><b>Economic</b>            Significant impact upon global economy means that public funding will be further constrained.            The rapid expansion of digital services and e-commerce as a result of COVID-19 has shifted crime online.            There is opportunity to develop new, innovative and sustainable ways of working that help us keep pace with our partners.</p>
	<p><b>Social</b>            There has been a rapid shift to living and spending time in the virtual world creating an increased risk of criminality.            Over reliance on technology and digital services leads to increased susceptibility to cybercrime – 20% of internet users in Scotland have experienced cyber fraud or computer misuse.            We need to adapt how we are visible in and accessible to online communities, promoting proactive prevention and resilience.            Prevalence of cybercrime is not reflected in reporting.</p>		<p><b>Technological</b>            The accelerated development and use of technologies has increased cyber threats.            Increased cybersecurity threats have prompted organisations to reinforce their information security systems and consider advanced analytics platforms.            Failure to invest in our infrastructure will mean we unable to keep pace with criminal networks.</p>
	<p><b>Legal</b>            As technology continues to develop, we must ensure that human rights and privacy rights form the foundation of any work to adopt or adapt technology and software for policing purposes.             Achieving the right level of engagement with partners and communities is paramount to ensuring we operate transparently and ethically.</p>		<p><b>Environmental</b>            Using outdated and less adaptable technology and software acts as a barrier to using resources effectively, and operating in a more environmentally conscious manner.             By procuring new, more efficient technology we can reduce our consumption of energy, reducing the organisations carbon footprint.</p>

Externally, the rapid pace of political, economic, societal, technological, legal and environmental changes set out above mean that we must continually adapt to meet the needs of the communities we serve.

Developments in technology are creating both challenges and opportunities for policing. Criminals are exploiting new technologies at an ever increasing pace, and a growing number of traditional crimes now also feature a digital element. The volume and importance of data and intelligence is also increasing, as are the opportunities and risks associated with its use. It is imperative that Police Scotland transition to be able to embrace current and future challenges and capitalise on opportunities that the digital age presents.

Police Scotland's strategic assessment and the Scottish Multi-Agency Strategic Threat Assessment (SMASTA) highlight the future threat from the widespread use of technology. Our latest assessment, aligned to our strategic outcomes, identified that protecting vulnerable people and tackling crime in a digital age are among the key policing priorities for the service.

Police Scotland recognises that the demands faced in policing are becoming increasingly complex and the resources available to meet these demands continue to be stretched. The creation of the internet and widespread use of digital technology has transformed the nature of crime, creating a new venue (cyber space) in which crimes can take place.

We know how important a visible police presence is to the public. Very often when the term 'frontline' policing is used it is in the context of 'visible' traditional street patrols in our communities. However,

the reality is that front-line policing also involves colleagues working in less obvious, but no less important, areas such as public protection, major crime and intelligence which are increasingly cyber dependent and cyber enabled.

In addition to tackling traditional and visible criminality, we must find different ways to prevent, disrupt and respond to the ever more inventive and complex use of digital tools and new tactics, at times originating from beyond our borders.

The type of demand Police Scotland faces on a daily basis has been changing for some time. Our evidence shows that since 1991, there has been a significant fall in certain traditional crime types. This trend has continued over the past 10 years, with overall crime decreasing by 27% since 2009-10. Fraud and crimes with a cyber element have, however, in the same period increased significantly with crimes of fraud increasing by at least 17% since 2009-10. Fraud is the most commonly experienced crime within the UK, partly due to increased access to the internet and internet-connected devices, and significant automation of fraudulent campaigns.

This is reflected in the Scottish Crime and Justice Survey (SCJS) where, of a range of crimes asked about, people were most commonly worried about cyber fraud. One in five adults who use the internet said they had experienced one or more types of cyber fraud and computer misuse in the year 2018/19, with one in twenty having been victims of more than one type. 50% of adults were worried that someone would use their credit card or bank details and 41% of adults were worried that their identify would be stolen.

Only a small proportion of property and violent crime in 2018/19 had a cyber element, however, 67% of repeated incidences of stalking and harassment are mostly experienced by electronic means, including text and online.

Another crime type that has been exacerbated by the internet is the sexual abuse of children. In the past the availability of child sexual abuse (CSA) imagery was limited, however with the growth of online communications and social media, it is relatively easy to access. Recent reports highlight the very concerning volume of online imagery<sup>1</sup>, some 8.3 million images were added to the Child Abuse Image Database in four years to 2019. The number of industry referrals regarding CSA imagery to the National Crime Agency (NCA) increased from 1591 in 2009 to 11,948 by 2018. The number of UK victims identified from sexual abuse imagery has also been rising.

During the COVID-19 pandemic, Police Scotland recorded a higher number of online child sexual abuse crimes in June 2020 than in any other month on record.

There were 530 online child abuse crimes recorded between April and June, with 226 in June alone. This is an increase of 21% against the same period last year and 34% higher than the five year average. Fraud crimes have also been rising steadily over the last five years but the ongoing pandemic has created further new opportunities to exploit changes in living and working conditions and the enhanced reliance on technology.

The NCA's National Strategic Assessment of Serious and Organised Crime (2020) also highlights the opportunities technological advances and the dark web provide for offenders to communicate, and to commit and conceal crime. The NCA assesses that the 'bar to entry' has lowered in recent years.

**"Today's criminals can sell firearms, livestream the abuse of children, or commit cybercrime or fraud from anywhere in the world, communicating covertly through encrypted services and moving illicit finances at speed.**

**"Trends identified in 2018 have become more prevalent during 2019, including the increased criminal use of encryption tools, the dark web and virtual assets, which refers to technologies such as Block chain, Bitcoin, crypto assets and virtual currencies."**

**National Crime Agency's National Strategic Assessment of Serious and Organised Crime (2020)<sup>2</sup>**

<sup>1</sup> Public Safety and Security in the 21st Century: the Police Foundation

<sup>2</sup> National Crime Agency's National Strategic Assessment of Serious and Organised Crime (2020) <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020/file>

The SCJS highlighted that there is significant under reporting of some crime types, particularly cyber fraud and computer misuse, as the majority of victims confirmed that they did not report the incident they experienced to the Police. This was particularly true in the case of scam phone calls and viruses, with 84% and 79% of victims respectively not reporting such incidents to anyone. Online theft of a bank card or bank account details was the type of cyber fraud and computer misuse reported by most victims (74%). Of this, 95% of online banking thefts crimes were reported to banks/credit card companies, while only 8% were ever reported to the police.

The UK Government Department for Digital, Culture, Media and Sport (DCMS) Cyber Security Breaches Survey of UK businesses and charities (March 2020) found only two-fifths of businesses (38%) and charities (42%) reported their most disruptive breach externally, with bank/building society/credit card company, internet service providers and customers mentioned more often than police.

Despite the under reporting levels set out, there has been a 100% overall increase in cyber investigations between July 2019 and July 2020 in Police Scotland, placing significantly increased levels of demand upon our existing policing model, capacity and resources. July 2020 saw 337 crime reports created in relation to cybercrime, with a significant proportion of these being described as fraud. In addition, increases in complex areas of criminal investigation are a real challenge for policing services already stretched in our capacity and capabilities. This is particularly acute where cases require examination of large volumes of digital evidence.

These changing demands are a reflection of our society, and where the communities we serve choose to spend their time, which is increasingly on virtual platforms.

Prevention and safeguarding work in this space is essential to ensuring we support, and offer guidance to those who inhabit these spaces. Through engagement with communities we will strive to promote awareness of these threats, and cultivate their ability to identify and manage them safely. This will support us to fulfill our duty to safeguard our communities, and take steps to identify and protect those at greatest risk of victimisation.

We must also focus our attention inwards so that our own resilience is empowered to deal with threats. As we strive to become a centre of excellence in cyber, ongoing development of our cyber resilience will ensure we are in a position to safeguard ourselves and our data. Leading by example will give us a strong platform to support efforts to establish Scotland as a cyber informed, and resilient nation.

Having recognised the increasing risk of harm from cybercrime and the ongoing shift in demand. It is clear that we must take steps to reshape the model of policing used in Scotland to one that is more proactive, agile and that understands technology to be simultaneously a challenge, and a solution.



# Our vision and objectives

The ambition of this strategy is to bring about the comprehensive change necessary to become a centre of excellence in digital and cyber policing. By exploring the different elements of our organisation, we have developed our objectives and designed enablers to direct our transformation.

# Police Scotland Cyber Strategy: Keeping people safe in the digital world

<p><b>Strategic outcome:</b> Threats to public safety and wellbeing are resolved by a proactive and responsive police service</p>		<p><b>Strategic objective:</b> Keep people safe in the physical and digital world</p>	
<p><b>Cyber Resilient</b></p>		<p><b>Cyber Investigation</b></p>	
<p><b>POLICE SCOTLAND RESILIENCE</b> Police Scotland is resilient and can respond to continually shifting threats</p>	<p><b>PUBLIC HEALTH, PARTNERSHIP AND PREVENTION</b> Holistically and sustainably prevent cybercrime using public health and partnership approaches</p>	<p><b>INVESTIGATION OF CRIMINALITY</b> Scotland is a challenging place for cyber criminals to operate</p>	<p><b>PROTECTION AND SAFEGUARDING</b> Our focus on protection and safeguarding remains at the forefront of all we do</p>
<p><b>Achieving this objective will mean that:</b></p>			
<p><b>Priorities</b></p> <ul style="list-style-type: none"> <li>Police Scotland has a holistic, robust and flexible approach to cyber security</li> <li>our systems and toolsets are modernised and underlying technologies are securely configured and protected</li> <li>we can evidence cyber maturity, maintain public confidence, enhance partner engagement and empower our people</li> <li>we work constructively and collaboratively with all sectors to secure Scotland's cyber resilience</li> <li>with partners we use a whole system approach to identifying and creating solutions to respond to threats and prevent crime and harm</li> <li>we have strong, established, relationships with key partners, sharing vital expertise, insight and experience</li> <li>Police Scotland is a visible and effective presence online, offering support and reassurance to victims and the vulnerable and successfully pursuing offenders.</li> <li>Our operating model has evolved and is prepared to address threat, harm and risk wherever it exists</li> <li>our investigative and intelligence capabilities have been enhanced, making use of all available training, technology and partner services</li> <li>we have ISO accredited, modern digital forensic services that are victim focused, ethical and keep pace with technological developments</li> <li>we use recognised and approved digital technology to safeguard people at risk of harm online</li> <li>we monitor, understand and respond to trends and behaviour changes in online activity using all available data sources</li> <li>we will share appropriate information with trusted partners and sectors, taking a collaborative support approach to protecting those who may be identified as vulnerable</li> </ul>			
<p><b>Enablers</b></p>			
<p><b>Respecting rights</b> Build trust and confidence by involving the public, communities and business as we design our approaches to tackle cybercrime.</p>	<p><b>Capacity and capability</b> Adjust our policing model to meet the needs of the public, communities, and businesses in Scotland</p>	<p><b>Infrastructure</b> Focus on transformation and investment in our infrastructure priorities to enable an efficient and effective policing service</p>	<p><b>Data driven innovation</b> Promote and develop our relationships and culture to drive innovative solutions that enable our cyber strategy</p>
			<p><b>Investment</b> Use our existing resources with targeted spend to save investment to achieve our cyber strategy objectives</p>

# Cyber resilient

We must be proactive in our approach to cyber threats. This includes within our own organisation and by providing support to the communities and businesses of Scotland. We will capture digital opportunities to keep people safe and enable Police Scotland, the public and organisations to proactively recognise and respond appropriately to cyber incidents. With that comes a requirement to build cyber resilience to prepare for, withstand, recover and respond to deliberate attacks or accidental events in the digital world. Police Scotland, with partners, supports resilience across all sectors, dynamically assessing the threat to the country, organisations, individuals and our own organisation.

The successful implementation of this objective will mean that Police Scotland is a cyber resilient organisation with the ability to continuously defend itself and others from digitally enabled harm, as well as working effectively with partners to support Scotland to be a cyber resilient country.

# Police Scotland resilience

Achieving this objective will mean that:

- Police Scotland has a holistic, robust and flexible approach to cyber security.
- our systems and toolsets are modernised and underlying technologies are securely configured and protected.
- we can evidence cyber maturity, maintain public confidence, enhance partner engagement and empower our people.

In Realising Scotland's full potential in a digital world: a digital strategy for Scotland<sup>3</sup>, the Scottish Government highlights the ambition that our critical national infrastructure, including emergency services, is secure and resilient against cyberattacks.

Our role is to keep people safe, whether that is in the physical or the digital world. In order to do this we must ensure our own cyber and digital security is robust and progressive.

All organisations and businesses have a duty to protect their service users, employees and customers. However, the consequences of the police service failing to protect our systems, technology and data are severe, and puts at significant risk the safety and wellbeing of our people, our partners and our ability to inspire continued trust and confidence by the public we serve.

We must address historic underfunding, outdated systems, and make sure that we have the structures, management systems, foresight and skills in place that will safeguard our service into the future. By using skilled officers and staff and by improving the infrastructure,

both technologically, in our data and working with external partners, we will be able to streamline our working practices. This work will realise financial benefits but also improve wellbeing, and create a more balanced, agile workforce with a culture of innovation.

Now, more than ever before, it is important that our people have a good understanding of cyber resilience and online safety. Our officers and staff should have the knowledge to be able to apply cyber resilience principles in both their home and work life allowing them to set an example for the communities we serve.




Since the publication of our DDICT strategy in 2018, we have made some progress, however we have been limited in how much could be achieved due to budget constraints and limited public sector funding to partners in a fast paced, continually evolving environment.

To ensure we can continue to effectively work towards achievement of the Scottish Public Sector Cyber Resilience Framework we are enhancing our approach to cyber security.

<sup>3</sup> <https://www.gov.scot/publications/realising-scotlands-full-potential-digital-world-digital-strategy-scotland/>

## Cyber security strategy

The strategy sets out our route to progress our capability and capacity in this area using the following five areas of focus: Assist, Detect, Assess, Protect and Transform (ADAPT).

ADAPT	
<p>Assist</p> 	<p>Cyber security cannot be provided through technology alone. Training and security awareness are crucial for employees. Secure supplier and partner engagements are another primary requirement to ensure safe and reliable communication can occur.</p>
<p>Detect</p> 	<p>To secure our assets and data, it is imperative that we have visibility and knowledge of them. Ironically, one of the pillars of security and confidentiality, can work against this requirement and impede visibility.</p>
<p>Assess</p> 	<p>Measuring the maturity and effectiveness of our cyber security is fundamental in identifying limitations and the opportunities to develop and improve.</p>
<p>Protect</p> 	<p>Robust cyber defence will be created through layered levels of appropriate, risk-based security controls, supported by increased skilled resources to manage and validate them.</p>
<p>Transform</p> 	<p>Technology in the modern world changes at a rapid pace, bringing both opportunity and risk with it. Current security paradigms can be strained or incompatible with these agile, interconnected technologies and require constant modernisation in order to remain effective.</p>

The ADAPT approach will provide a holistic, robust and flexible approach to our own internal cyber security. It will allow Police Scotland to safely modernise our systems and toolsets, whilst providing the assurances required that the underlying technologies are securely configured and protected. It will provide opportunities for Police Scotland to evidence cyber maturity, maintain public confidence, enhance partner engagement and empower our people.

Cyber Security is built around the principles of providing Confidentiality, Integrity and Availability of digital systems and data. In real terms this means that systems and data should be consistent and tamper-proof, accessible when needed and only viewable or modifiable by authorised personnel.

There is no simple solution to achieving this within a complex organisation like Police Scotland with a structure of 20,000+ users, 23,000+ network-connected devices across 500+ locations; especially when considered against a backdrop of multiple potential threat actors ranging from state sponsored and organised criminal groups to individual disaffected employees.

The accepted method of tackling these issues is by incorporating security at multiple levels, using a variety of techniques, layering solutions on top of each other to provide an overlapping, multi-threaded, cohesive security blanket; a technique commonly referred to as "defence in depth".

By building these layers of security we provide broad resilience through a range of countermeasures that may be activated if any single control or level is compromised.

ICT activity in relation to internal cyber security and risk mitigation will continue to focus on the adoption of relevant new technologies and resource capacity that will enhance our cyber resilience, close existing identified gaps and ensure sound cyber security is in place to underpin the continuing transformation programme across Scotland. The continual development of our capabilities will expand on existing security controls by introducing new technologies that provide greater visibility of the internal Police Scotland ICT estate, allowing greater detective, responsive and preventive security actions to be performed.

The cyber security and resilience focus broadly covers the following areas:

- **perimeter defences** – continually evolving our perimeter controls to maximise the return on investment delivered by current controls and additionally to support new controls to assure the technical security of our key system and information assets.
- **network access control** - controlling access and identify threat across wired, wireless and VPN network.
- **internal defence** – use of a suite of detective controls to enable the identification, visualisation and analysis of cyber incidents within our ICT perimeter, addressing the 'insider threat' risk and enabling a proactive approach to the disruption of malicious activity.
- **cyber incident response** – continue to expand our capability to respond rapidly to significant cyber incidents and malware propagation.

- **cyber investigation** – utilising a suite of investigative tools and appropriate resources, provides the capability and capacity required in order to appropriately investigate cyber incidents on Police Scotland infrastructure.
- **be aware and prepare** – run regular user awareness sessions in relation to cyber security and undertake regular exercising of our cyber resilience plans including simulating attacks to test our defences.

Given the complexity and extent of Police Scotland's digital infrastructure, coupled with a diverse array of constantly evolving threat vectors and new technologies. It will never be possible to provide 100% assurance in relation to the organisation's cyber resilience, nor should it be thought that a single point in time project will rectify all future cyber security requirements.

We will continue to put a focus on the defence and resilience of our information systems and data assets, building on our defence. Our in-depth strategy will improve our overall security capability and support moving us from a reactive posture to a position of active cyber defence. This will ensure that Police Scotland remains at the forefront of cyber defence capability in the UK public sector.

# Public health, prevention and partnership

Achieving this objective will mean that:

- we work constructively and collaboratively with all sectors to secure Scotland's cyber resilience.
- with partners we use a whole system approach to identifying and creating solutions to respond to threats and prevent crime and harm.
- we have strong, established, relationships with key partners, sharing vital expertise, insight and experience.

We must be less reactive to cyber threats in Scotland's communities and organisations, shifting our focus to proactive prevention. To do this in a sustainable and effective way, we will work with our partners, encouraging agile ways of working and sharing expertise that benefit all sectors. This will include exploring and developing new, innovative solutions in terms of cyber resilience and cyber investigation.

By using a public health approach, we can ensure that cyber enabled and cyber dependent crime are treated in a holistic manner, with a focus on prevention, collaboration and sustainability.

A whole system approach is fundamental to the success of this objective. This model will be used to innovate new solutions in partnership, using a tried and tested structure which our partners understand.



## Prevention

Our preventative approach focuses on early intervention and early resolution to help build resilience in the vulnerable communities we serve. Our Cyber Harm Prevention Team work to develop and deliver interventions at national and local levels. By doing so we improve outcomes and help Scotland become a digitally resilient nation.

We will work to align with the Scottish and UK Governments in their approach to proactively supporting national infrastructure, individuals, communities and partners to embed resilience and prevention. Our ambitions in this space can make us a critical enabler in ensuring Scotland is safe, secure and prepared to meet the short, and long-term needs of our businesses and communities.

This will include extending our presence into the digital world, developing and co-creating appropriate interventions and increasing awareness of digital threats. Building the resilience of vulnerable people and communities is key to safeguarding those susceptible to repeat victimisation.

Supporting those with vulnerabilities will remain at the forefront of our preventative approach. The rapid shift to digital services has meant that some groups, such as older people, have experienced digital isolation. The Scottish

Government has committed to tackling digital poverty by supporting digitally excluded people get online by providing both devices and internet connections. With this commitment, we must be aware of the increased threat to some vulnerable groups and ensure we work with communities and partners to ensure we proactively prevent risk and harm.

We will also improve our preventative approach through the better use of data and ensuring security products are secure by design. This will be enabled by embedding our whole system approach to prevention across Police Scotland, including the creation of the Partnership and Prevention Delivery Unit to lead our overarching public health approach.

Police Scotland cannot achieve this preventative approach in isolation. We will work with current partners in collaboration and continue to develop new strategic partnerships. We will be flexible and dynamic in how we partner with others, creating new relationships and opportunities for collaboration.

## Cyber prevention in schools

In the last year a local high school made contact with the Cyber Harm Prevention Team for support in relation to escalating concerns regarding sexting and the sharing of nude pictures among pupils, and its struggle in putting a stop to it. During the review of this matter by the team, it was determined that it was only a matter of time before some of the pupil's behaviours exposed them to serious risk of harm. Through engaging closely with the school the team:

- Developed a letter addressed to parents/carers highlighting the risk and harm that these activities can cause in the short, and long term.
- Presented at school assemblies that allowed the team to address over 900 pupils in a single day to offer guidance and raise awareness of the potential harms these behaviours can cause.

This focused approach ensured that those most at risk were supported, while the wider school and families were made aware of the harm and risk associated with these activities. The school were highly appreciative of this work and credited it with making a positive difference in preventing real-world repercussions of harmful behaviour.

To understand and keep at pace with the digital threats we face and the means for tackling them, we will work closely with UK and International policing and security partners, academic organisations and industry leaders to develop our proactive and reactive capabilities. This includes developing and embedding the technology and data we need to prevent and disrupt cyber dependent and cyber enabled criminality. Realising the benefits of shared data, analysis and insights, using innovation in line with our data protection obligations will inform our collaborative approach and optimise our impact.

### **Partnership**

Police Scotland recognises that strategic partnerships are vital to enabling the changes we seek to undertake. Only through utilising the support and resources of public, private and third sector organisations can we achieve this. It is clear that partnership, both who we partner with and how we do this, becomes an enabling aspect of this strategy, allowing us to redefine how we tackle cyber issues.

## Immersive Labs

Immersive labs are a UK based cyber training organisation, specialising in using “gamified” learning to simulate live cyber environments and threats. The NPCC have funded and procured licences for this labs for use by policing, of which Police Scotland has received in surplus of 100.

What we plan to do:

- Roll out the immersive lab program across key specialist areas and local policing, providing essential training and skill development.
- Identify Cyber Champions to be assigned product licences and access to support networks. These individuals will form a nationwide network that will act as a point of contact for investigators and local divisions to receive guidance and support for managing cyber incidents.

Rolling out this training represents a significant opportunity to provide essential training that will support the development of digital knowledge and skills, as well as professional development. This will also bolster our capacity and capabilities by empowering greater levels of resources to handle cyber incidents, with a more accessible national support network to support this work. We are credited with making a positive difference in preventing real-world repercussions of harmful behaviour.

We are committed to developing a partnership and collaboration framework that places agile connections and innovative ideas at its core. By adopting a whole system approach, we will work effectively with partners to identify and understand the problem, thereafter providing support and capacity to design and test strategies to address it.

This will be led by the Partnerships and Prevention Delivery Unit to enhance local and national approaches to partnership working.

Providing the right opportunities and routes into the organisation for people with the skills and knowledge we need is also a key objective. This will directly

support the ongoing development of our capacity and capabilities, and enhance our ability to safeguard communities.

Making the best use of our officers and staff member’s skills is of key importance to supporting our ongoing work, and transformation goals. Our recent Cyber Champion initiative has helped to give us greater insight into the specific experience and talents our people possess, which are not currently being utilised to their full potential. With this work we can begin to map these skillsets, and ensure these individuals are supported with opportunities to make the most of their expertise, and apply their skills across the organisation.

## Building capacity and capability through partnership working

### Public sector



Strengthening our relationships with other public sector organisations we will help create more capacity for Police Scotland. Working in close collaboration with our public sector partners, we will create campaigns and initiatives to provide the public and organisations with the knowledge and resilience to understand what the threats are, and how to deal with them.

### Academia



By creating links with universities and research bodies we will create mutually beneficial relationships that allow for the sharing of research and operational knowledge. This form of collaboration will also create new pathways for officers and staff to enrol on bespoke courses to develop their skills in areas that are of vital importance to the future effectiveness of the organisation.

### Private sector



Much of the content and platforms that individuals and organisations routinely use and rely upon are created and sustained through the private sector. The private sector as a whole finds itself a frequent target of cyber-attacks. We will seek to explore new opportunities for collaboration with industry leaders in order to reduce instances of victimisation and revenue loss.

## Public sector

In working with the Scottish Government and other public sector partners we will develop partnerships, ensuring that the safety and wellbeing of the communities we serve are at the heart of them. By strengthening our relationships with other public sector organisations, we will create more capacity to share vital information to better understand current threats and those on the horizon. With an accurate picture of the scope of cybercrime and those affected by it, we will empower each other to take steps to enhance our defences, and stay ahead of a changing threat landscape.

This will ensure we can:

- work in close collaboration to create campaigns and initiatives to provide the public and organisations with the knowledge and resilience to understand what the threats are, and how to deal with them.
- collaborate and develop safe, informative and accessible spaces for the public to engage with us and find the correct source of the support they need.
- engage with the public to advertise new campaigns, share local information and provide access to learning materials to safeguard our communities from the most pressing threats.

## Academia

One of the main challenges of tackling cybercrime is that it is constantly evolving and adapting, along with the platforms and digital environments that enable it. Leading academic research is focused on cyber security and the threats it seeks to repel. By creating the right links with universities and research bodies, we will create mutually beneficial relationships that allow for the sharing of research, insights and operational knowledge, and provide opportunities for:

- students to interact with our processes and data to support the ongoing development of cybercrime/security as a field of research.
- collaboration to create new pathways for officers and staff to enrol on bespoke courses to develop their skills in areas that are of vital importance to the future effectiveness of the organisation. This will also provide access routes for prospective students into the organisation who traditional recruitment models may not be suited to.
- academic partnerships to develop bespoke learning packages and curriculums that will support our campaign of increasing digital literacy and skillsets.

## Private sector

Just as we have partners who support our work in the physical world, we need to build partnerships that enhance and support our ability to protect those who increasingly live within digital networks and communities. Many of the platforms and content that individuals and organisations routinely use are created and sustained in the private sector, a frequent target of cyber-attacks looking to disrupt their systems and exploit their users.

Collaborations with private companies, such as banks, have enhanced our information sharing to reduce instances of victimisation and revenue loss.






We will seek to build upon this work and explore new opportunities to:

- collaborate with private organisations, such as leading technology and software development companies, to keep pace with emerging criminality and develop preventative interventions to safeguard those who are most vulnerable to harm, where possible by design.
- increase information sharing to allow the development of more in-depth, and ethical analysis of the data we hold. By increasing our understanding, we can design new services and processes that can be created to tackle the issues and demands that our analysis presents.
- develop innovative solutions co-operatively with the private sector to provide the public with increased level of safeguarding from potential threats, along with more accessible resources and communication channels to seek information and support.

# Cyber investigation

Cybercrime continues to rise in scale and complexity as a global threat. Cyber dependent and cyber enabled crime transcends across many areas of criminality in Scotland, and poses significant threats to our National Security. The capability and impact of Hostile state actors cannot be understated<sup>4</sup> as this can be seen to transcend their activities into serious and organised crime.

This threat and form of criminality has been advanced by serious organised crime groups (SOCG) who commit, or facilitate, a wide range of criminality, including economic cybercrime; child sexual offences and indecent images of children; cyberstalking offences; cryptocurrency; and digitally enabled criminality and services to cause maximum impact, disruption and/or financial gain.

Nature of Cybercrime in Scotland	
 <p><b>Sexual offences</b></p>	It is estimated that approximately 30% of cyber offences recorded by Police Scotland between 2019-20 were sexual offences.
 <p><b>Financial &amp; economic offences</b></p>	4.8% of internet users in Scotland have had an online account accessed for fraudulent purposes, with half (50%) of adults in Scotland worried about their bank/credit card details being used to obtain money, goods or services.
 <p><b>Computer Misuse Act 1990 offences</b></p>	1% of incidences of device infected by malicious software reported to Police, with 30% going unreported because it was felt the matter was too trivial and not worth reporting and 22% believing that police do not deal with this sort of incident.
 <p><b>Threatening behaviour &amp; communication offences</b></p>	Repeated incidences of stalking and harassment are most commonly experienced by electronic means, including online.
 <p><b>Procurement of illicit goods and services offences</b></p>	Online storefronts such as Gumtree and eBay, as well as sharing and selling groups on social media, are commonly used to sell illicit goods. This includes illegal fireworks, cigarettes, illegal streaming services and counterfeit clothing.

<sup>4</sup> 2017 Wannacry attack on the National Health Service, for example.

## Investigation of criminality

Achieving this objective will mean that:

- Police Scotland is a visible and effective presence online, offering support and reassurance to victims and the vulnerable and successfully pursuing offenders. Our operating model has evolved and is prepared to address threat, harm and risk wherever it exists.
- our investigative and intelligence capabilities have been enhanced, making use of all available training, technology and partner services.
- we have ISO accredited, modern digital forensic services that are victim focused, ethical and keep pace with technological developments.

Our priority is to make Scotland a challenging place for criminals to target or operate. Transforming our response to cybercrime is an ongoing and significant challenge that requires investment. Our model of policing has to change to enable us to expand our specialist services alongside an increasing and vital shift to embed local cyber-capabilities.

We know that our ability to exploit data and harness new technologies will be fundamental to adapt our approaches to investigation to respond effectively to societal and criminal trends around digital.

Policing needs to navigate existing and emerging technologies and consider the overall impact they will have on investigations on an ongoing basis.

Advances in technology will have varying degrees of significance as they are adopted and mature which requires our investigative approach to continue to be agile, flexible and able to adapt to shifting priorities and demands.

### Our policing model

The model for operational policing in Scotland has historically been based on tried, tested and valuable approaches to address traditionally committed crime in the physical space. Our demand information has, over a period of time, highlighted significant changes to the role of policing in Scotland. We are proactively developing capability to inform our understanding of the threat which was often unseen via previous methods. The key changes involve the significant influence of cyber and internet technology and the role of policing to support the most vulnerable in our communities.

While some progress has been made to adjust policing approaches and resourcing over time, there is a need for a significant shift to a sustainable, agile model to meet public and community needs, currently and in future.

The model will include a focus on policing in the digital space, designing our specialist services, aligning resources to meet demands and upskilling local policing.



## Visible policing in the physical and virtual world

We know how important a visible police presence is to the public. Very often when the term 'frontline' policing is used it is in the context of 'visible' traditional street patrols in our communities, however, the reality is that frontline policing also involves colleagues working in less obvious, but no less important, areas such as public protection, major crime and intelligence which are increasingly cyber dependent and cyber enabled. The work undertaken across Specialist Crime Divisions and at police offices across the country is vital for the safety of the public in the physical and virtual world.

Police visibility can also be considered in terms of our online presence, including through social media, and we will continue to increase our visible presence online to support communities and deter criminal activity both on the surface and dark web.

Our online 'reach', in essence how many people see our communications messages, is increasing, as are how many people and accounts share and respond. We have a digital first approach to our communications so that the public and media can directly access the information and safety guidance that they need.

The Police Scotland's Public Contact and Engagement strategy addresses how we need to increase the ways in which people can contact us for help or advice, which will extend the online options available.

We will increase our connectivity across the web so that people are able to easily connect to us in as few steps as possible and in the way that best suits them. We will continue to introduce new ways for people to provide us with information, data and footage.

### Case study

In 2020 we introduced Major Incident Public Portal (MIPP), a website to give the public access to various forms in the event of a terror attack, major disaster or a high profile incident such as a murder.

It allows people to send information, reports, images and video footage directly to the police casualty bureau and major incident teams.

Police Scotland used MIPP when appealing to the public for information regarding the death of Emma Faulds in Ayrshire and the Shona Stevens homicide inquiry in North Ayrshire. It is updated with live investigations and is promoted when witness appeals are issued.

<https://mipp.police.uk/>

We will work with policing partners and platform owners on online safety to improve ways that people and companies can easily report and address issues, problematic behavioural trends and suspicious and malicious activity. We also recognise and respect that some people do not necessarily want to engage directly with policing, but are no less vulnerable online. We will work with partners to ensure that safety guidance can be provided and reports can be made through trusted routes, and that criminal and intimidating behaviour is not missed.

## Specialist policing support

There is a requirement to develop a resource and delivery model that addresses cyber and internet crime as one of our highest strategic priorities. This model requires the functionality and adaptability to be able to receive and assess intelligence in volumes never before experienced; identify threats that contain the highest risk, and mitigating opportunities to meet and eliminate the threats posed.

The increasing levels of intelligence in relation to cybercrime requires more resource to assess, and leads to more cyber investigations and digital forensics activities. Cyber marked Intelligence logs have risen from 80 in January 2018 to 723 logs in January 2020.

In addition, digital forensic demands continue to increase at pace. This is due to criminals being found with more electronic devices, which also have considerably more data storage capability, impacting on law enforcement ability to pursue and disrupt these offenders.

Online Child Sexual Abuse and Exploitation (OCSAE), for example, is an area of criminality that continues to increase and develop its modus operandi in targeting and exploiting those in our communities that are most vulnerable. The cyber environment is enabling this activity to be shared by criminals across the world with 'off the shelf' malware and technical tools which allow the less technically proficient criminals to commit cybercrime.

We will design, develop and deliver enhanced specialist service and online capabilities, with effective local policing support for Police Scotland to respond

to this ever increasing threat. Cyber dependent crime, and our ability to disrupt organised criminal groups/ individuals who are advancing into the cyber landscape for economic gain, whilst creating hardship for our communities, are presenting the greatest challenges for policing at present.

Our officers and staff will require to be agile and innovative against an increasingly technically sophisticated criminal community. It is vital that we support our officers and staff so that they have the knowledge, guidance, training and equipment necessary to tackle these areas with confidence, to support our communities and partners in policing and criminal justice.

With investment in cybercrime and its interdependent functions, we can enhance our understanding of the threat, allowing us to develop both a reactive and proactive response to cyber related crime.

To create a National Centre of Excellence and meet existing demand levels in our communities, we will require a significant uplift of officers and staff. This will build our capacity in all key areas such as cybercrime intelligence, investigations, research and development, innovation, assurance and digital forensics.

The proposed model would provide a specialist policing service to the public, communities and businesses of Scotland which will make it increasingly difficult for criminals to commit cybercrime.

## Policing in local communities

We will build on the progress made by our Digitally Enabled Policing programme to enable local policing to provide a range of support and services to the public and communities at the first point of contact, in all areas of the Scotland – Island, rural, remote and urban, taking into account local needs and circumstances.

Ensuring local policing is fully equipped with the technology and skills needed to investigate, without the requirement to await specialist support in some cases, is critical. This will assist Police Scotland to manage demand levels, as instances of cybercrime continue to significantly increase at local level, and provide greater support in our communities every day.

Our most recent cyber incidents data highlight this growing demand for support in our local communities:

- 583 incidents with a Cybercrime Tag or Qualifier were recorded in July 2020, up from just over 200 in January 2020.
- Crime reports were created for over 57% of these 583 incidents in July.
- 61% of the incidents in July related to Fraud.
- Communications offences (113) and Abduction/Extortion/Sextortion (33) were the next most common crime types.

Our priority will be the creation of dedicated functions for investigators to access specialist advice and guidance 24 hours a day, 365 days a year. This will increase confidence and accuracy of information provided to victims, witnesses and even suspects.

The design and development of our policing model set out above are a critical element of our approach to tackle cybercrime.

The following areas are also critical areas of focus as we seek to enhance our approaches and improve our policing services.

## Reporting

This strategy is aligned to our Public Contact and Engagement Strategy, which outlined our vision to increase public safety and wellbeing by making it easy and safe to report a crime or other incidents, get information and feedback, enabled by digital services.

While we will continue to respond to 999 and 101 calls, we will create a more accessible, inclusive and seamless public experience, enabled by digital services such as online chat and referral.

Due to the borderless nature of cybercrime, it is important to have an overview of the wider context of cybercrime affecting the UK. To simplify and enhance the cyber incident reporting experience for victims and those involved in responding to incidents, we will work with the National Cyber Security Centre (NCSC) to develop a cybercrime incident reporting portal. This will allow organisations to report cyber incidents in a timely and effective way, streamlining their reporting process. This will form part of a joint effort to respond to cyber incidents and keep the UK safe.

A high proportion of cyber incidents are not reported to the police or our partners, so our priority will be to increase the proportion of incidents that are reported.

We will continue working with the Scottish Business Resilience Centre (SBRC) and others to encourage businesses to introduce technologies which automatically identify and report attacks on their systems, generating intervention activities by Police Scotland and our partners. This removes the burden from small and medium sized businesses in particular, which may not have the dedicated resources at their disposal to identify such incidents, while eliminating confusion over who they should report to and allowing them to focus more on their core services. The introduction of a Cyber Incident and Response Manager will mean that SBRC will work with key stakeholders to develop a single point of contact cyber incident triage service and provide support to all businesses in Scotland .

For the public, communities and businesses, this all means only having to report incidents once, in ways most suitable to them, reducing the frustration of being passed between agencies and departments. Incidents can then be dealt with early, reducing the risk of continued or escalating harm. They will be able to contact us through a variety of digital channels, submit multimedia evidence and self-serve if desired for appropriate low-risk situations.

Despite these improvements to how people can interact with us, the response will be consistent, no matter the reporting method.

## **Intelligence**

The increased use of technology to commit or enable criminality, has removed all geographical boundaries and does not respect international jurisdiction.

In order for Police Scotland to be a key partner in combating cybercrime we need to aspire to be recognised across UK and global intelligence, law enforcement and industry partners that we are able to not only investigate but collect, assess and disseminate high quality intelligence that will allow us to establish strategic worldwide intelligence sharing partnerships. Key partners include NCA, Interpol, Europol, NCSC and international Law Enforcement agencies.

There is an opportunity to use digital technology much more effectively to complement our own judgement and analysis of threat, risk and harm. New technology will ensure we can rapidly and precisely address the risks of harm of offending, including when digital channels are a core element of our overall exposure.

An Interpol report from August 2020 on cybercrime and the impact of COVID-19 highlights that “cybercriminals are developing and boosting their attacks at an alarming pace”. The breakneck speed, scale and constantly evolving nature at which many cybercrimes now occur mean that it has never been more important for us to acquire systems and adopt processes that will enable us to sort through much more data, at pace and respond effectively.

The public, our communities and businesses should rightly expect that our systems enable the timely sharing of information with our partners in the global fight against cybercrime. This will be our priority for Intelligence, but will require more investment to overhaul our intelligence systems and processes.

## Identification

Appropriate digital tools will support policing to rapidly identify behaviours that can lead to harm, ensuring we can target interventions appropriately and at pace. Transformational research continues in relation to the Dark Web to fully support this development of digital tools.

Where appropriate, digital capabilities can help us to identify and be involved where people are at risk of harm or of offending. The Child Abuse Image Database (CAID) remains a significant investigative and intelligence source for Police Scotland and continues to develop and support the critical and high risk area of child sexual abuse. Our strategic direction around child sexual abuse images and other key areas takes full account of the HMICS recommendations and will provide a sustainable and effective future approach.

Police Scotland will also be better informed and more effective in our local policing approaches amongst the public and communities of Scotland.

We will use technology to provide better information. The introduction and development of apps, coupled with the increasing connectivity of mobile devices will continue to improve the effectiveness of our officers and staff. This will increasingly help officers and staff to assess their environment, potential threats and items of evidential value in real time.

Our priority will be to keep our officers and staff safe, informed and enabled by digital tools that allow them to identify threats and respond appropriately.

## Disruption and Intervention

We will increasingly use digital tools to disrupt criminal activity, to identify the potential for harm to large public groups, volume and scaled online threats and serious organised crime groups who are seeking to exploit technology.

Digitally enabled interventions have the value of working across boundaries. These include online pro-activity, design, development and adoption of technologies that support automated data sharing and analysis tools.

Specialist staff and officers within Police Scotland need more capacity to proactively target and identify offenders through technology. This requires working with partners, in a safe, streamlined manner which will ensure we can avoid duplication of effort and enhance the public service provided to all our communities.

Our priority will be training more of our people to use the digital tools at their disposal to disrupt all forms of criminality at all levels, creating a hostile environment that will deter offenders.

## Detection

Digital and technological investigative capability will be enhanced by building and upskilling a workforce with the skills and knowledge to ensure that we are appropriately equipped to provide investigative services.

By establishing an agile, efficient, resilient and secure technical infrastructure we will enable our people to capitalise on advanced and emerging technologies increasing asset capability, digital product quality and facilitate more intelligent and effective data analysis.

Our richer intelligence picture, better tools, collaborative approach and highly trained people will be more able to identify, detect and prosecute those involved in cybercrime.

The quicker we can gather and evaluate evidence following crimes or attempted crimes enables us to more readily and effectively identify the perpetrators.

Currently, nearly all investigations have a digital element. Mainstreaming the cyber skills of those in first contact with victims, witnesses and suspects, when supported by the right tools and access to specialists, will increase the likelihood of offences being detected and offenders being brought to justice. The recently implemented 'Cyber Champions' cadre within Police Scotland has identified a significant degree of skills and experience in the cyber arena that has previously not been explored. This will be of significant benefit to the specialist officers deployed to investigate high level cybercrime but also provide support and guidance to Local Policing to upskill front line staff.

When determined criminals are not deterred in spite of our efforts to prevent crime, safeguard the vulnerable and disrupt criminal activities, detection will remain our last resort.

Our ability to prevent and disrupt cybercrime will be supported and enhanced by our approach to detection and pursuing offenders. The quality of our detection aligns with Detect themes and outcomes of Scotland's Serious Organised Crime Strategy and the Pursue element from the Contest strategy.

Our priority will be to bring a higher proportion of cyber-offenders to justice and improve outcomes for affected victims.

## **Dark web**

Whilst most cybercrime occurs via the surface web, or what would generally be described as the internet, there is another part of the internet, known as the dark web, which is increasingly used to commit crime, often on an industrial scale. The dark web is not visible to search engines like Google and is accessed through an anonymising browser called Tor.

Common crimes arranged via the dark web include the supply of commodities (e.g. controlled drugs, counterfeits, firearms, data) and trafficking of human beings. It facilitates other cybercrime, such as extortion, fraud, ransomware attacks and livestreaming of sexual abuse. The proceeds of such criminal activity is laundered using cryptocurrencies. This often involves organised crime groups, criminal networks and terrorists, who are increasingly working together.

We will share technical expertise and intelligence with national and international law enforcement partners to unlock the evidence held on encrypted devices used by criminals to coordinate and plan their activities. It is essential that we adopt a global approach with our partners to cracking encrypted global communication services which are often used exclusively by criminals.

Our priority will be to increase our dark web presence and investigative ability. We will, proactively deploy specialists to enable a greater assessment and understanding of the threat to our communities. Our trained people will be part of a network of global law enforcement specialists that can work together to share knowledge and tactics to tackle dark web criminality effectively, with increased ability to unlock evidence on encrypted devices and networks.

## Digital Forensics

Digital forensics is a key area of forensic science and includes the identification, recovery, investigation, validation and presentation of facts regarding digital evidence found on digital storage media devices.

The prevalence of this digital evidence across a broad range of crime types is ever increasing. Subsequent pressures and demands on digital forensics also resulting in a need to ensure we have an agile, future focused operating model to enable policing investigations in the medium and longer term. Our current demands levels indicate in 2020 even with the impact of COVID-19 Police Scotland are still receiving on average nearly 1000 devices per month.

Growth in the use of digital technology has led to significant demand pressures in this area of policing. This results in delays to devices being examined, resulting in backlogs to investigations, impacting victims, witnesses and suspects waiting for the outcome and often the return of their devices. The delay also increases the risk of harm as offenders are not brought to justice at an early stage. With increased activity, threat and risk from CSAE this demand is only likely to increase moving forward.

Digital examinations present a complex challenge due to the variety of devices, increased end-to-end encryption, the emergence of new communication platforms and apps coupled with access to vast amounts of remote data storage via the cloud at a relatively inexpensive cost to the user. We need to develop new techniques, exploit new technologies, work closer with our criminal justice partners, simply to maintain our capability to extract and analyse information.

Recent high profile international investigations has seen the potential impact that can be delivered when technology is deployed to overcome the tools used by criminality. In Scotland alone Joint Operation Venetic has seen the recovery of in excess of £25 million of controlled drugs, £7 million in laundered cash, notwithstanding the firearms also recovered during the investigation. The investigation has impacted on the majority of organised criminality and Scotland and greatly enhanced our understanding of the scale of the threat posed to our communities.

It is crucial that we maintain public trust and confidence in policing. Whilst the public is broadly supportive of the police using digital forensic analysis, recent issues around disclosure and consent for digital device examinations, means people are more aware of the issues involved. As we develop new ways of working we will protect the rights of the communities we serve and embed our values into everything that we do.

Building on recent progress to introduce digital triage to local policing to support operational expediency and digital evidence gathering, Police Scotland has commenced the process towards obtaining an appropriately accredited ISO standard digital forensic laboratory by 2022. This will be the most significant piece of work undertaken by Digital Forensics since the formation of Police Scotland and will require significant investment across the digital forensic infrastructure.

A range of benchmarking activity is underway with SPA Forensic Services and more widely across the UK to enhance our understanding of the requirements and benefits.

This information will enable us to develop a framework for achieving the accreditation. In broad terms the accreditation will require addressing of key areas of digital forensics, including;

- Estate
- Training
- Hardware
- Software
- Recruitment and realignment of existing and/or specialist skilled personnel

Each of these areas will require varying degrees of design, development and investment and be underpinned by consistency in process and governance to ensure sustainability against the standards set by the accreditation.

A quality framework is also being developed for non-forensic aspects of digital investigations including triage technologies within the same timescale.

The delivery of an enhanced business assurance structure and accreditation of our digital forensics to an internationally recognised level will ensure we have a competent, robust and consistent capability for the future.



# Protecting and safeguarding

Achieving this objective will mean that:


- we use recognised and approved digital technology to safeguard people at risk of harm online.
- we monitor, understand and respond to trends and behaviour changes in online activity using all available data sources.
- we will share appropriate information with trusted partners and sectors, taking a collaborative support approach to protecting those who may be identified as vulnerable.

Section 20 of the Police and Fire Reform (Scotland) Act 2012 provides that one of the duties of the police is to protect life and property. This duty to protect is embedded in our core role and is woven throughout every aspect of police training through to operational delivery.

Online connections and communities can be a lifeline for many people, particularly those who may experience isolation in their everyday lives. Earlier in this strategy we described how we will work with partners and play our part in Scotland's cyber resilience. This section considers how, as a police service, we will protect and safeguard individuals and communities at particular risk of harm and exploitation. Protecting and safeguarding means protecting adults and children at risk of harm and abuse. Under the Adult Support and Protection (Scotland) Act 2007 there is a statutory duty on police to refer any adult who may be at risk of harm to the council and to work with councils to protect the adult's safety and wellbeing.

We do this with partners through understanding vulnerability, anticipating risk, engaging with people, providing advice and guidance, ensuring tools and mechanisms are accessible to individuals and their support networks, and as a police service, by being accessible and available and primed to intervene or respond if required. Where a certain threshold is reached in relation to wellbeing and harm we have statutory responsibilities to act and follow statutory processes.

The upcoming United Nations Convention on the Rights of the Child (UNCRC) bill will see a renewed commitment to embedding the rights of children, and young people in Scottish law. This ambitious piece of legislation will create more support mechanisms and legal protections for young people, ensuring their voices will be heard and their rights upheld.

99% of 16-44s are online everyday	Smartphones are the most popular internet-connected device, used by 78% of UK adults. Many of us may use more than one	9 in 10 people access the internet in the home (2018)
62% of time spent on the internet is through mobile devices		54% of adults aged 65+ shopped online in 2019
Almost two-thirds of households now have mobile broadband access	Smart speaker usage has grown 98% since 2017	Agile, flexible and remote working has increased, changing how we interact

Digital participation is increasing across nearly all demographics and the Scottish Government is aiming to improve digital participation across Scotland's communities as one way to reduce social exclusion and economic inequalities.

The Carnegie UK Trust<sup>4</sup> identified a correlation between digital exclusion and a wide range of factors associated with social exclusion, and that the internet is associated with better mental health and wellbeing, when all other factors are accounted for, with those with internet access less likely to have lower than average mental health than those who do not have internet access.

Each new platform, application and technology opens up new opportunities for users, but also new risks to their security, safety and wellbeing. Digital poverty can also mean that whilst people of all ages may be able to get online, they are less likely to have access to security solutions that offer them protection from being targeted by criminals, malware and harmful and distressing content.

<sup>4</sup> [Digital Participation and Social Justice in Scotland](#) Carnegie UK Trust

## Recognition

Safeguarding adults and children includes being vigilant to and identifying when they may be manipulated, intimidated, at risk of harm or being harmed, both physically and mentally. Often this takes place in private, which has extended into the digital realm meaning that spaces that may traditionally have been seen as safe, may no longer offer protection from known, or unknown, threats.

Relationships can be quickly established online, many of which are genuine, and some of which are not. Like other forms of abuse and bullying, the child or adult may be coerced or intimidated into concealing threats, injury or mental abuse by people they know, strangers, and increasingly, fake and hidden profiles. Police and other key partners in social care, education and health must be able to understand the new ways in which someone may come to harm, which can change rapidly as can the language that may be used to describe these interactions.

## Understanding the scale

We will work proactively with regulators, current and new providers and justice partners to encourage and embed mechanisms into online platforms, including social media and gaming, to increase the likelihood that concerning and illegal content will be reported to moderators and the police.

We will use all available data sources to monitor and understand trends and behaviour changes in online activity.

Those with less online access are also more likely to have regular interactions with health, social care and other public services, provided directly or indirectly, with sensitive information held as a result. They are also more likely to access loan and credit services through less reputable providers.

We are increasingly spending more time online and sharing more of our personal data through internet enabled devices such as smart phones wearables e.g. smart watchers. Patient monitoring through 'health tech' is becoming more prevalent for those in need of long-term care, which includes people who do not otherwise use technology to get online. As this increases, here is a risk that people are sharing more personal data than they realise and that data breaches may be more likely to have a personal impact to wellbeing.

Without appropriate support and constructive intervention, the future prospects of these children and young people may be damaged, and skills and talent lost to the workforce.

## **Effective technology**

We will use recognised and approved digital technology to safeguard people at risk from crime in the real world as well as from cybercrime. Behavioural detection, data analytics and machine learning will allow us, with partners, to swiftly identify triggers and patterns.

## **Working together**

Online platforms can disproportionately provide opportunities for abuse, bullying and intimidation. We recognise that there are groups of people communicating with others who do not want to interact with the police, even if they are at identifiable risk of or experiencing harm. We will work with providers so that there is visible access to advice and support, and a safe route to report issues, helping to build trust with the police service.

We will actively work with the NCA's Child Exploitation and Online Protection (CEOP) command, and be guided by its principles to inform our approach to online child exploitation.

We will work with those who have responsibility for protecting others so that they have the right information they need to keep those in their care safe. We will share appropriate information with trusted partners and sectors, taking a collaborative support approach to those who may be identified as vulnerable.

We will also work more closely with financial services to more proactively identify potentially vulnerable people who may fall victim to online threats. By doing so we will be able to provide collective safeguarding and assistance to prevent repeat victimisation and provide better support.

# Our enablers

Our objectives are supported by five enablers. By bringing these elements together as we progress to implement our strategy, we give ourselves the best opportunity to successfully achieve our objectives.

## Respecting rights

Employing a rights-based approach to policing, that prioritises privacy and protection is critical. Public and stakeholder engagement will enable us to understand this as we consider how we develop and implement technology to support policing in Scotland.

We will protect the rights of the communities we serve and continue to embed our values into everything we do. Fairness, integrity, respect and human rights will continue to be our guiding principles as we aim to improve our cyber capacity and capability.

We will only use new technology and approaches where there is strong ethical oversight, transparency and based on the outcome of public engagement and conversation. For this, we will embed the following supporting structures:

- Values and ethics framework. Enabling us to teach, observe and measure our credibility, values and behaviours, and see the impact of our actions.
- Service standards and principles. Embedding quality and consistency of service to manage, meet and exceed public expectations.
- Public and community engagement. Involving and engaging the public and stakeholders to gain their confidence and trust.
- Academic research and worldwide experience. Using the latest research evidence and lessons.

Our executive and leaders will be supported in decision-making with robust, real-time insights and feedback to improve their understanding and respond to evidence that can stand up to scrutiny. This will be done by establishing an independent Ethics Panel to provide regular, objective and independent input to Police Scotland to ensure that we are getting the balance between privacy and protection right.

The Scottish Parliament has passed legislation to introduce a national Biometric Commissioner, expected to take post in 2021, to oversee and hold policing to account in managing biometric data such as finger-prints, DNA samples and other new technologies that may be introduced in future.

### **Building public confidence and trust**

Public and stakeholder trust is critical and involves accountability, education and providing the right service for the public and communities we serve. Policing is about people and policing by consent. We will involve and engage to do things 'with' the public and stakeholders rather than 'to' or 'for' so that the way in which we use tech and our approaches are acceptable, beneficial and gain confidence. In undertaking consultation, we will adhere to the guiding principles set out in our Public Engagement Framework for ensuring our consultation is representative, inclusive and ethical.

Through a rights-based policing model we will work to strike the right balance between privacy and protection as we consider our approach to tackle cybercrime and our investment in both technical surveillance and digital forensics. Maintaining the consent of the people will be our foremost priority to any work and decisions made to ensure we are not only maintaining, but enhancing public trust and confidence in our activities.

### **Infrastructure**

In order to achieve our objectives we must look to improve our infrastructure, ensuring it is fit for purpose now, and in the future. Our infrastructure underpins and supports operational policing across Scotland. However it has been recognised and, highlighted in our DDICT Strategy, that areas of Police Scotland's infrastructure require improvement. This includes making vital changes to our ICT and data infrastructure.

In order to achieve our objective we must invest. The right ICT is required to enable our preventative approach, including data sharing with partners. It is well recognised that our current ICT infrastructure no longer meets our needs and lags behind the infrastructure of other public sector organisations. Through utilising investment opportunities we will identify the most ineffective aspects of our infrastructure and procure replacements that enhance, not hinder our capabilities.

Modernising our systems and devices will allow us unprecedented access to information held on our systems, enabling ease of access and sharing capabilities. Big data analysis will develop insights into harm prevention, effective resource allocation, and create the foundation needed for use of predictive analytic software. Having improved and dynamic ICT will also serve to make our information sharing partnerships streamlined and accessible. Improved ICT will bring us in line with our partners and put us in a position that means we are able to efficiently address cyber threats.

## Capacity and capability

In order to achieve our objectives we must improve Police Scotland's capacity with regard to cyber resilience and cyber investigation.

Our capacity to identify and address cyber threats has limitations. We must look at ways to improve our capacity, including further developing our model for policing and key partnerships with public, private and third sectors, as well as investing in technologies that will support operational policing and streamline processes.

Our approach to building capacity will focus on a shift in our current policing model to allocate our resources where they can best meet the demands of the public, communities and business. Police Scotland is committed to investing in our officers and staff, ensuring we have the right skills, in the right place within the organisation.

We will create a national centre of excellence in cyber within the organisation to provide increased support for cyber inquiries, investigation and prevention work. Through this work we will deliver support, training, guidance to Local Policing to enable them to address a greater number of number of concerns raised on a day to day basis.

To build our capacity we need to both invest and re-align existing resources to meet demands. Our approach to transformation has been designed to support policing to build capacity in key areas that can be used to shift our resources to meet demands. Our change portfolio is supporting this as we implement Digitally Enabled Policing (DEP), Contact Assessment Model (CAM) and a range of contact

options set out in our Public Contact and Engagement strategy and as we follow the direction being set by our strategic workforce plan. As capacity is realised our current change portfolio and similar work to transform corporate support services will identify capacity amongst our staff and work streams. With this we will adjust our policing model and assign our overall resources to most effectively meet demands.

Our strategic workforce plan highlights that the proactive recruitment of technical staff and apprentice level entry staff will deliver a sustainable policing model moving forward, with a career path for the most capable staff blended with operational experience.

An incremental increase will mean that the resource model continues to develop its capability and agility to make it nationally and internationally renowned in law enforcement and industry. Cyber criminals will find Scotland a much more challenging environment to operate in.

To meet our overall requirements we will adopt a phased approach, fully aligned to strategic workforce planning, ensuring our cyber commitment is reflected throughout the plans for the organisation, in order to meet the changing demands of policing in Scotland. This will involve both an uplift in officer and staff numbers in SCD and embedding cyber skills within local policing.

## Phase one

Re-alignment of resources and capacity will commence. Initially, a significant number of officers and staff will be re-aligned to support the new Cyber Centre of Excellence and build the infrastructure for local policing to tackle an agreed range of cyber offences.

Additional work will also begin to analyse our data and create a clearer picture of the scope of cyber crime and its demand on the organisation.

## Phase two

In year three roles will have been created and filled, based on the updated demand information, by officers and staff to further bolster our investigative and preventative capabilities. Local policing will be taking a leading role in tackling instances of cyber enabled crime, ensuring a high level of service and support for communities and businesses. Our internal data will be used to ensure our resources are allocated effectively, and identifying key areas for further research and preventative work.

## Phase three

By year five there will have been a significant number of officer and staff roles created within the organisation and a step change enhancement in our capabilities. Through creating clear pathways and development opportunities we will have nurtured a workforce with a diverse set of qualifications, experience and knowledge, establishing Police Scotland as a centre of excellence in cyber. These individuals will provide a source of unparalleled support and expertise in matters of cyber investigation, resilience and prevention,

accessible to the whole organisation. Combined with clear analysis of our data, and local policing divisions empowered to tackle certain instances of cyber criminality, we will meet the demands of modern policing, and be adaptable for future challenges.

## Capability

In order to achieve our objectives we must build on Police Scotland's cyber capability. We must deliver an internationally renowned response, with capability delivered through providing the right training and tools to our officers and staff across the service, and thus begin to strengthen our investigations, resilience and prevention capabilities.

A significant shift is needed within Police Scotland to invest in, attract and develop the data and technology talent we need to transform our approach to cybercrime investigation.

We will require to define the right roles and have the right resources in the right place. To do this effectively we need to implement a new data and technology talent model that is flexible and adaptable to meet the demands and pace of ongoing digital change and its impact on criminality.

A new competency model will be required to enable the change in core activities to deliver the skills shifts needed to support cybercrime investigation in both specialist support areas and local policing.



We will design and develop a future-focused operating model for digital forensics. With the support of the Cyber Capability Programme, we are currently working to review digital forensics so that the service is supported in the journey to accreditation.

Only through providing the right training and tools for our officers and staff across the whole service can we begin to bolster our capability. By upgrading essential training we will embed the skills and knowledge to empower the whole organisation to play a role in combating increasing levels of cyber and cyber enabled criminal activity.

We are currently working with academic partners to ensure that our people have the right skills and knowledge to address cyber threats of all types. The Digital and Data Skills Academy (DDSA) will deliver bespoke training packages on cybersecurity, cyber investigation and digital skills. This will not only support the personal development of our officers and staff, but will also help us embed digital and data skills across the organisation.

## Digital Policing for the Future

### Phase 1



Current

The DDSA is a collaboration between Police Scotland and Glasgow Caledonia University (GCU) to deliver a bespoke package of free training on cybersecurity, cyber investigation and digital skills. This will support those with an interest / or who are working in these areas to develop their knowledge and technical skills.

### Phase 2



Development  
12-18 months

Through refinement of the training curriculum the academy will continue to support the development of those who have a keen interest in cybersecurity / investigation areas. More emphasis will be placed on the creation of accessible courses that improve digital literacy and basic skill development across the organisation.

### Phase 3



Future model  
3-5 years

Through close collaboration with our partners, coupled with analysis and adaptation of delivered courses the academy will offer different tiers of bespoke training to staff/officers that caters to the needs of the organisation. This will support local policing through enhanced probationer training, more support for operational staff, and increased professional development opportunities.

Another way we are looking to upgrade existing training delivery is through Virtual Reality Technology. Utilising virtual reality platforms we can enhance our learning environment with the ability to train for situations that would otherwise be logistically challenging. These platforms will provide officers with the opportunity to learn in realistic dynamic situations, taking account for operational movement and actions that are expected of officers, ensuring they are better prepared if and when placed in such scenarios.

We also recognise there are further opportunities to stimulate learning through the use of mobile devices, enhancing the devices to enable interactive learning and development support on the go will allow officers to access important information and learning scenarios at all times.

The Cyber Champions initiative is illustrative of this, whereby staff throughout the organisation have volunteered to become involved to enhance our capability across the organisation. We will invest in them through a blend operational and interactive learning, mentoring and support.

We will also consider opportunities to identify talent at an early stage and channel those skills in a positive direction. We will develop partnerships with higher education and industry in order to introduce the right specialist talent into policing. The development of these partnerships will allow us to explore opportunities to work with schools, develop apprenticeships and graduate opportunities. In doing so we will meet our workforce skills requirements and provide new and unique career pathways.

Cultivating strategic partnerships will be vital to ensure we have access to up-to-date knowledge of threats, harm prevention and individuals with the right expertise for policing in Scotland.

### **Data driven innovation**

Police Scotland will continue to promote and develop an innovative culture, working closely with partners from public, third and private sector organisations to identify opportunities and threats, collectively seeking innovative solutions to support our aspirations in cyber.

The data we hold will be instrumental in facilitating the level of change this strategy requires. Work is already underway to maximise opportunities to record and collect data that is high quality and suitable for review by our analysis functions. This work will directly support our ability to accurately assess changing demands, and create solutions to resolve, and prevent them. To support this we must commit to continuing our work on developing clear governance channels that have the right mix of leadership skill. Supported by ethical frameworks to provide clear operating parameters, balancing operational risks with citizen rights and privacy.

We will continue to collaborate, understand shared problems and share appropriate information to meet requirements of legislation with due consideration of both privacy and ethical considerations.

Through implementing these functions, we will be able to use our data to support innovation, and turn opportunities into tangible sustainable solutions, transforming the pace and success of delivery from years and months to months and weeks. Embracing new technology will continue to provide opportunities to enable policing in Scotland to efficiently deliver in areas of priority, supporting policing to work with the public, communities and business to design and improve services. These approaches will support Police Scotland to embrace new technology and systems by testing and evidencing digital solutions and opportunities that will keep us sustainable and fit for the future.

## **Investment**

In order to achieve the change outlined in this strategy, additional investment will be required across the service. Delivery of the strategy will ultimately produce cashable, efficiency and social benefits. So far as is possible, benefits will be realised through changes to our policing model (aligned to strategic workforce planning) improved capability and capacity and more efficient processes, however a mix of capital, revenue and reform funding will also be needed.

In September 2018 the Scottish Police Authority approved the Digital, Data & ICT (DDICT) Outline Business Case (OBC) put forward by Police Scotland, which included proposals for investment to address the growing demand from cyber dependent and cyber enabled crime.

However, the requested funding has not been forthcoming, and demand has continued to grow. It recognised that underfunding has constrained our approach to cyber, including the intervention and disruption that would prevent and reduce the impact of crime. With the lack of resource we are unable to confidently assess the threat to often the most vulnerable in our community. New technologies will enhance our ability to respond to increasing demand, but this has to be together with increased numbers of skilled officers and staff, and investment in training and innovation.

Our DDICT strategy described the priorities, projects, budget, staffing and related initiatives needed to transform our digital, data and ICT capability, with alignment between all our technology programmes. Two years on, the blueprint will be assessed to identify any gaps or additions required to support the implementation of this strategy.

This coordinated approach will create a roadmap but allow for local transformation activity. This will be supported by technical design capability, with a pragmatic approach to using commercially available 'off the shelf' applications rather than creating complex, bespoke solutions, unless genuinely required.

We will move towards open source code for mobile applications used in policing, and formalise our development standards. Along with enabling interoperability with a larger range of partners and trusted suppliers, this will drive suppliers to work towards similar high standards.

Working with others, we will explore piloting and testing of emerging connected technology, for example, drones, sensors, and heads up displays. This will maximise the potential of emerging technologies and improve sharing in the UK and internationally of knowledge whilst avoiding duplication of effort and costs.

We will embed our data strategy in the approach to implementation ensuring we drive data quality and consistency, facilitate systems integration and data aggregation, enhance sharing mechanisms and improve access to data between Police Scotland and partner organisations. By creating a high performing data culture with optimal data quality and availability, we will ensure data is used, acquired and shared in an ethical manner to maintain public confidence and trust in policing.

We will build national automation, analytics and Artificial Intelligence (AI) capabilities to enhance data quality, facilitate data sharing across key systems and extract insights that support evidence based policing and better outcomes for the public and communities.

Unlike the public sector environment, the rate of invention and change in the criminal sphere is not limited by complex financial governance or accountability. We recognise that to effectively keep pace with and counter new threats, we will need to be able to adapt quickly to introduce new functionality and capability. We will require streamlined, but robust, approval and governance processes that allow innovative solutions to be rapidly introduced at the point they can be most effective and provide best value.

The additional investment required for implementation of the strategy will be set out in more detail in the overarching implementation plan. Where possible, additional officer and staffing costs will be met from within existing resources as the policing model adapts and work to transform corporate support services is completed, freeing up capacity for cyber. The requirement for additional funding and investment will be based on continued monitoring of the levels of threat, risk, harm and demand.

# Strategic alignment and performance

This strategy supports the direction of both the Scottish Government and the UK Government, including the Scottish Government's Cyber Resilience Framework and Catalyst Programme. These articulate our role in proactively supporting national infrastructure, individuals, communities and partners to embed resilience and prevention, and responsibilities.

At the UK level, the National Cyber Security Strategy 2016 to 2021 describes the approach of government, security services and policing to building resilience. The National Police Chiefs Council (NPCC) is responsible for the Digital Policing Strategy 2030, focused on the digital transformation of policing in England and Wales.

This Cyber Strategy has been developed taking into account the complex cyber landscape and new developments across Scotland, the United Kingdom and

beyond. We must meet industry standards with aspiration to create nationally and internationally renowned capability, ensuring credibility across law enforcement and critical partners across the world.

It is aligned to our Joint Strategy for Policing (2020), Policing for a Safe, Protected and Resilient Scotland.

The Joint Strategy highlighted our need to transform Police Scotland's capacity and capability to prevent, disrupt and respond to the ever more inventive and complex use of digital tools and new tactics by criminals. The development and delivery of this cyber strategy are key steps towards achieving the strategic outcomes and objectives of the Joint Strategy.

It complements Police Scotland's wider plans and enabling strategies, such as Digital, Data & ICT, Transforming Corporate Support Services, Public Contact and Engagement and Estates.

Our Annual Police Plans (APP) and supporting delivery plans will enable the delivery of the Cyber Strategy. The Cyber Strategy is aligned to the APP which outlines how we will improve our support services to enable delivery of local policing; promote the health, safety and

wellbeing of our people and develop and maintain the right crime and specialist support services for policing in Scotland.

The following diagram shows how this strategy fits in Police Scotland’s strategic planning framework.



## Performance framework

Police Scotland uses an outcomes-focused performance framework, again aligned to the strategic outcomes and objectives of the service that run through our strategies and plans. The framework describes how we will monitor and measure progress on our strategic outcomes and objectives.

This includes benchmarking data to allow us to assess the performance of our approach against other police services, and comparable public and private sector approaches.

## Impact measures

A range of qualitative and quantitative performance indicators will be measure to show progress as follows:

Evidence of cyber markers being utilised to identify and record cybercrimes	Evidence of improved understanding and responses to cybercrimes
Development and adoption of other engagement routes and channels	Improving relationships between young people and police
Evidence of participation on community engagement initiatives	Evidence of using feedback and insight to improve services
Level of confidence in Police Scotland	Level of trust in Police Scotland
Improving understanding of threat horizon	Impact from national prevention campaigns
Evidence commitment to investment in technology modernisation	Increased development opportunities provided and undertaken by staff and officers

# Governance

Police Scotland has an established Cyber Resilience and Digital Investigations Board (CRDIB). Chaired by the Deputy Chief Constable Crime and Operations, in addition to senior leaders and specialists from within the service, membership also includes representatives from the Scottish Government, Scottish Police Authority and key partners.

The board oversees and provides assurance on Police Scotland's strategic and operational response to cyber, ongoing activity to enhance our own resilience and capability, and our contribution to the delivery of the Scottish Government's Cyber Resilience Strategy and Public Sector Action Plan to improve cyber resilience within the communities of Scotland. CRDIB will drive and monitor our progress against this strategy and reports into the Strategic Leadership Board.

Police Scotland will also report progress to the Scottish Police Authority to the appropriate committee and the Authority Board as required, including through performance reporting outlined above.



