SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Agenda Item 2.3.2

Meeting	**SPA Policing Performance Committee**
Date	**15 June 2023**
Location	**Microsoft Teams**
Title of Paper	**Policing in a Digital World Programme & Rights Based Pathway Pilot**
Presented By	**ACC Andy Freeburn**
Recommendation to Members	**For Discussion**
Appendix Attached	**Yes - PDWP Overview and Rights Based Pathway Presentation**

PURPOSE

The purpose of this paper is to provide members with an update on progress and direction of the Policing in a Digital World Programme, which includes the creation/development of a Rights Based Pathway, to ensure robust processes in terms of the introduction of technology in Policing. This is to ensure a focus on human rights compliance, key ethical considerations and maximising stakeholder engagement and communication.

This paper will specifically provide a progress report in relation to:
Agenda item 2.3.2 – Policing in a Digital World Programme

Members are invited to discuss the contents of this paper.

1. BACKGROUND

1.1 Police Scotland's Cyber Strategy 2020 '*Keeping People Safe in a Digital World'* was approved by the Scottish Police Authority (SPA) on 30 September 2020.

1.2 The PDWP has a clear aim to transform how Police Scotland respond to the evolving threat of cybercrime. The Programme will enable us to continue keeping Scotland's people, communities, businesses and assets safe in both the physical and virtual world.

1.3 The Programme has embedded a 4P's approach to dealing with cyber related threats (Pursue, Protect, Prepare and Prevent), in line with the NPCC led 'Team Cyber UK' methodology.

1.4 It will enable Police Scotland to:

- Focus on an improved victim experience (overarching outcome).
- Deliver an effective investigative response (Pursue).
- Target local cybercrime prevention messaging (Protect).
- Work to identify and divert people vulnerable to engaging in cybercrime (Prevent).
- Engage with businesses and organisations to help them develop effective measures to mitigate threats and risks associated with cybercrime and, where appropriate, engage in testing and exercising (Protect).
- Develop Centres of Excellence and provide guidance to the wider force, helping mainstream cyber skills and knowledge into most areas of policing (4P approach).

1.5 By ensuring all officers and staff on the frontline and in specialist roles have the knowledge, skills, tools, and support to confidently and effectively tackle cybercrime Police Scotland will be better equipped to prevent, respond to, and investigate such crimes; we must build the workforce and tools to keep people safe in public, private and virtual spaces.

2. FURTHER DETAIL ON TOPIC REPORT

Current Threat Picture/Drivers for Change

2.1 Cybercrime is an area of increasing risk and Police Scotland must ensure that our policing model can respond effectively.

2.2 The following figures provide the scale of the problem and the threat, risk and harm this poses to the communities across Scotland:

- 511% increase of Online Child Sexual Abuse and Exploitation (OCSAE) referrals from 2015-2021.
- 650% increase of referrals regarding child sexual abuse imagery over a 9 year period.
- 68.2% increase of fraud over last 5 years.
- 17% decrease in fraud detection rate.
- 95% of fraud now online and synonymous with cybercrime.
- In 2022/23, 16,879 crimes of fraud were reported in Scotland, which equates to an average of 46 cases per day.
- It is also recognised that this crime remains hugely under-reported.
- Around 40% of businesses across the UK are victims of cybercrime, some of whom will not have reported it.

Progress to Date (Overview of 2022/23)

2.3 ***January 2022* -** PricewaterhouseCoopers (PwC) reviewed Police Scotland’s current cyber capabilities and provision, benchmarked the organisation against UK and international standards and assisted with developing a number of deliverables such as:

- Critical Friend Review of the Cyber Strategy.
- Cyber Target Operating Model.
- Capability Assessment.
- Presentation Products.
- Strategic Outline Business Case.

2.4 During this period, the PDWP and PwC teams came together and approached this piece of work as “one team”. PwC subsequently reported that the Strategy provided a clear strategic ambition and intent for Police Scotland, assessing that overall it is fit for purpose in setting the conditions for implementation.

2.5 Using a capability model PwC produced a high level Target Operating Model (TOM) and a costed Strategic Outline Business Case (SOBC).

2.6 ***July 2022 Change Board*** - Following approval through the PDWP Programme Board and the Portfolio Management Group (PMG), the SOBC was presented at Change Board, from which there was broad support from members, recognising the critical importance for Police Scotland increasing its cyber capability and capacity.

2.7 ***18 October 2022 PDWP Programme Board*** – To prioritise the implementation programme, ACC Freeburn the SRO directed that 'Prevention, Pursue and Partnerships' were to be the key focus over the next financial year and highlighted the potential of a number of low cost options that could make a huge difference, add value and help protect Scotland from cybercrime.

2.8 ***30 November 2022 DCC Crime and Operations Management Board (COMB)*** – ACC Freeburn presented an update to COMB, where attendees were invited to note the paper and endorse/support the ongoing work to date and future proposals of the Programme, whilst being invited to offer any comment and advice to assist in shaping Police Scotland's commitment in this area.

2.9 ***6 December 2022 SPA Briefing Session –*** DCC Graham and ACC Freeburn attended this and provided updates to the membership around deliverables, dependencies, timelines, programme resource requirements/status and finance.

2.10 ***7 December 2022 SPA Policing Performance Committee*** – ACC Freeburn presented a high level overview and update in relation to PDWP which was well received by the Committee and were supportive of the intention/direction of the Programme. There was an agreement that Police Scotland should embrace and implement new technologies whilst appropriately ensuring safeguards, standards and human rights consideration. It was agreed that ACC Freeburn would bring proposals back to the Committee in June 2023.

2.11 ***27 January 2023 Policing in a Digital World Professional Reference Group –*** In addition to the PDWP Programme Overview and associated priorities, the concept of the Rights Based Pathway in terms of introducing technology into the organisation presented to the Group which was supported with associated feedback that helped shape the process.

2.12 ***17 February 2023 Policing in a Digital World Programme* Board –** Overview of the Programme, identified priorities and planned deliverables through the various projects outlined to the SRO and members. CAID FM technology was also presented and approved by the Board with the proposal to introduce as part of the Rights Based Pathway Pilot.

2.13 **14 March 2023 Audit and Risk Board** - This gained further support at the Audit and Risk Board, when presented by ACC Freeburn, supported by the Head of Strategy & Innovation and the Chief Data Officer.

2.14 **23 March 2023 Portfolio Management Group (PMG)** - The Rights Based Pathway was presented at the Portfolio Management Group (PMG) where it was supported.

2.15 **4 April 2023 Change Board** – The Rights Based Pathway was presented and endorsed by members.

2.16 **12 April 2023 Strategic Leadership Board -** The progress and direction of the PDWP, the Rights Based Pathway and introduction of CAID FM was presented and approved.

FY 23/24 Budget Submission and Planned Deliverables

2.17 As outlined previously, the Target Operating Model (TOM) produced to fully deliver the Cyber Strategy.

2.18 The PDWP in fully recognising the current budgetary pressures, have reviewed the TOM with a view to identifying the most cost effective deliverables with a key focus on the following 3 priority areas:

Pursue

2.19 Recognising Police Scotland’s statutory responsibility to ‘Keep People Safe’ in the digital world and relentlessly pursuing those who seek to cause harm through cyber-criminality. This requires the enhancement of our capacity and capabilities, so that we equip our people with better tools, techniques, training and skillsets to impact against the highest online harms. We will therefore focus on improving our digital forensics capability and our response to Online CSAE and Fraud.

2.20 Linked to this is the recognition that continually adding more people is not a long-term solution and Police Scotland require to introduce new technologies to make processes more efficient. The inclusion of the Rights Based Pathway in this paper, will provide a mechanism to ensure that technologies introduced by Police Scotland have been assessed as legal, ethical and have the requisite safeguards and assurances around public safety and confidence.

Prevention

2.21 It is clear that as more crimes are being increasingly committed online and have a digital footprint, that Police Scotland will be unable to ‘arrest their way out of this problem’. Greater effort will need to be applied to ensuring that we do all we can to educate and inform the public on the threats and trends that are occurring in the digital world.

2.22 Through the sharing of intelligence and encouraging and supporting the public and businesses to maximise prevention, it is assessed that a significant quantity of cyber-offences could be reduced. It is recognised that this is not solely the responsibility of the police, which links to the following point around partnerships.

Partnerships

2.23 Police Scotland recognise that there are multiple agencies and organisations who have a footprint in cyber security, investigation and intelligence. This includes organisations such as Cyber Scotland and the proposed Scottish Cyber Coordination Centre (SC3).

2.24 There is therefore a need for Police Scotland to continue to collaborate across the entire cyber sector in Scotland, to pull together the collective resources, so that we become more than the sum of our parts. Cyber-criminality is an existential threat to us all and Police Scotland are appealing to the broader cyber community to become involved in a mapping exercise which will allow us all to understand the gaps and overlaps and where are collective efforts should be focused.

2.25 Police Scotland have already successfully proven the worth of such arrangements, through the creation of a Multi-Agency Fraud Hub, with the banking and financial sector to share information and solutions in the growing crime area of online fraud.

2.26 In line with the 3 priority areas, it is the ambition of the PDWP to deliver a variety of products and services across a number of projects, during the 2023/24 financial year. A draft budget proposal for the next 3 financial years has been submitted along with the associated proposed delivery plan.

Deliverables Financial Year 23/24

2.27 The work and products being prioritised for delivery during this period can be succinctly outlined as follows:

- **Cyber Training and Capability Pursue & Prevention (Pursue)** – This project enables the organisation to transform Police Scotland's capacity and capability to respond to the threats of cybercrime through the review and implementation of a full suite of cyber training products to officers and staff from basic to advance levels. The Initial Business Case was been approved at SPA Resources Committee in May 2023.

- **Digital Forensics Vans (Pursue) –** Approved at Change Board, March 2023. Four vans secured by fleet for this financial year, with kit-out and operational delivery estimated Q2 2023. The introduction of the vans allows for 'at scene' examination of digital devices, seized under warranted powers, therefore reducing the number of digital devices that would otherwise have been transported to be examined in the DF Laboratory, adding to existing heavy workloads.

- **Digital Evidence Detection Dogs - (Pursue) –** Business Justification Case being prepared for presentation at Change Board in July 2023. Recruitment and training expected to take approximately 12 months from business case approval.

- **Critical Issues (Pursue & Prevention)** –Text Analytical Solution for the Internet Investigations Unit (IIU) and visual text analytics functionality to improve effectiveness and efficiency. This will replace the current database which is unstable and cannot be utilised whilst also providing an analytical tool to the IIU Investigators.

- **Cyber Kiosk (Phase 2)** – Project seeks to design and deliver a solution that will allow connectivity of the 41 cyber kiosk devices to the IT network so that they can communicate with a central server to enable the sharing of management information only. This remote process will replace the current manual process, thus freeing up valuable time and associated costs. The networking does not allow the sharing of information between the kiosk devices. A project plan and costings for each site is in development. The PDWP are working closely with Digital Division to identify a pilot site that can be setup as a proof of concept subject to design sign-off.

- **ISO17025** – Project to deliver formal accreditation of all five Police Scotland Digital Forensics Laboratories. Work has commenced with the Digital Forensic Lab at Muggiemoss, Aberdeen with accreditation of all five labs expected by 2026. This project reports six monthly to the SPA Forensics Committee.

2.28 The Programme also possesses an emerging technology and horizon scanning work stream with the aim of delivering/enhancing the following:

- Dark Web search capability.
- Crypto Currency investigative, seizure and storage capability.
- Police Cyber Alarm - Product aimed at SME's, Business and 3rd sector partners to help strengthen their cyber protection capabilities.
- Prevent/Cyber Choices – Programme to enable Police Scotland to identify, engage and divert young and potentially vulnerable people who are on the cusp of cyber-criminal behaviours onto more positive pathways.

2.29 Now/Next/Beyond - Work ongoing to help establish and Research and Development (R&D) process. By fully understanding the problem we are trying to fix will help identify the solution/technology to fix/improve/enhance. This will form part of a future operating model horizon scanning / R&D function.

2.30 Cyber Futures – This work will develop the future target operating model for Cyber and Fraud in the organisation and the workforce mix required to deliver against this demand.

Current Partnerships

2.31 In terms of the importance around partnerships, the PDWP have identified and developed strong working relationships with a number of organisations across the Cyber landscape in terms of law enforcement, public, private, and third sector partners.

2.32 In harnessing these close working partnerships, Police Scotland is looking for ways to work more collaboratively and seamlessly together, whilst breaking down any remaining divisions that may exist across the public, private and the voluntary sector. With the common enemy of the cyber-criminal we recognise the formidable force we become, when we pull together our resources and expertise.

Cyber Scotland/Cyber and Fraud Centre (Scotland)

2.33 One of Police Scotland's key areas of collaboration in cyber is the Cyber Scotland Partnership. The Cyber Scotland Partnership is a collaborative leadership approach to focus efforts on improving cyber resilience across Scotland. The Scottish Governments key strategic stakeholders come together in a formal partnership arrangement to drive the delivery of activities that will achieve the outcomes of the Strategic Framework for a Cyber Resilient Scotland.

2.34 A key member within the Cyber Scotland Partnership is the Cyber and Fraud Centre (formerly SBRC). Their vision is to make Scotland one of the safest and most resilient places to live, work and run a business. They offer a range of services and guidance to people and businesses in the Prevent/Protect categories while educating and training those to become more resilient and better prepared to mitigate future cyber threats.

Scottish Cyber Co-ordination Centre (SC3)

2.35 SC3 was announced at Cyber Scotland Week in February 2022 and will seek to become a recognised, authoritative and collaborative function to combat the accelerating threat of cyber-attacks to Scotland, its businesses and people. The intention is to leverage better coordination and collaboration for the common benefit and so prevent and respond to escalating cyber risk in a more rapid and resilient way. SC3 will not seek to replace the National Cyber Resilience Centre or existing resilience structures. SC3 will collaborate with key stakeholders from Police Scotland , NHS National Systems Support, Hefestes (Education), Scottish Government (SG) I Techs and Digital Office (Local Authority) in delivering the mission of improving Scotland's capabilities to defend against, and be resilient to, the cyber threat. The co-ordination of this work formed part of the year one year discovery phase.

2.36 A Head of Centre (HOC) is to be appointed in due course and key work stream leads have been appointed and structures established to contribute and provide strategic direction for SC3 moving forward. The SC3 brand will be created along with on boarding of key partners who will support and assist in the development of the 5 key work-streams. In support of this activity, it is understood that a communications plan will be developed leading up to further SC3 milestones during Cyber Security month in October 2023.

NPCC Digital Forensic Portfolio

2.37 The vision of this business area is to improve operations through national oversight and coordination. In order to achieve this the portfolio will focus on key areas which align to and mirror PDWP objectives:

- Improve systems inter-operability and align with national programmes. Harness technological change and opportunities through effective partnership working.
- Meeting the data challenge through streamlining data management.
- Developing the workforce for consistency of standards and approach.
- Building trust and new robust capabilities
- Shared learning and collaboration through research and development.

Fraud Multi-Agency Hub

2.38 Fraud is synonymous with online crime and over the last 5 years this has seen a 68% increase, equating to an average of 1500 crimes per month, 95% of which is online. The policing response to these crime types has used 400,000 of investigation hours in the past 5 years.

2.39 ACC Andy Freeburn, as Chair of the Strategic Fraud Governance Group with partners from Scottish Government, the banking and financial sector and the Cyber and Fraud Centre Scotland, have commenced a multi-agency triage hub pilot, with the objective of ensuring that the public and private sector work more collaboratively to tackle and prevent this escalating threat.

2.40 The group meet on a weekly/monthly basis and report into the Fraud Strategic Governance Group, chaired by ACC Freeburn and has already achieved success in stopping live online offending and recovering victim's financial losses.

UK Fraud Strategy Alignment/Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS)

2.41 In terms of the wider UK approach, Police Scotland are also working closely with the City of London Police and assisting in the development of the new Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS), formerly known as Action Fraud. Police Scotland are not currently a member of this service, however are considering this position in light of the new developments.

The new FCCRAS has been designed with the following collective objectives for both the victim and law enforcement:

- Improved victim experience and satisfaction.
- Lead to criminal justice outcomes.
- Prevent crime and reduce harm.
- Contribute to an improved understanding of the threat from serious and organised crime.
- Improve systems inter-operability and align with national programmes.

2.42 This supports our alignment to the recently published UK Fraud Strategy, which outlines key actions across the following pillars:

- Pursue Fraudsters.
- Block Fraud.
- Empower People.

2.43 A Fraud co-ordination group is being established to coordinate all Fraud related activity in Police Scotland, to develop a national approach.

Governance

Police Scotland (internal)

2.44 All business cases for transformational change progress through the Investment Governance Framework. Each project reports to a Project Board, then Programme Board, progressing to Portfolio Management Group (PMG) and Change Board. The value and complexities of the project will determine the next/future governance steps, through SPA and Scottish Government.

Policing in a Digital World Professional Reference Group (external)

2.45 Police Scotland and the Scottish Police Authority's joint vision is to deliver comprehensive change to become a centre of excellence in digital and cyber policing.

2.46 Following publication of the Cyber Strategy, the focus has been on planning for implementation and engagement with stakeholders and the public.

2.47 The Scottish Police Authority is committed to supporting Police Scotland in building public trust through open and transparent discussion and engagement, promoting and supporting the need to build effective preventative partnerships and secure additional investment.

2.48 It is recognised that the strategy implementation and engagement plan will benefit from collaboration with key industry and public partners led by both Police Scotland and the Scottish Police Authority.

2.49 This will support strategic delivery, while offering informed expertise and effective challenge as Police Scotland progresses with implementation of this future focused strategy.

2.50 This resulted in the creation of the joint (SPA and Police Scotland) Policing in a Digital World Professional Reference Group with the inaugural meeting taking place on 22 September 2002. This was chaired by DCC Malcolm Graham and SPA Board Member Caroline Stuart, with representation from the National Cyber Resilience Advisory Board, Scottish Business Resilience Centre, Academia and the Equality and Human Rights Commission.

2.51 The positive discussions from the initial meeting helped set the agenda, inform the terms of reference and membership, helping to shape the direction of the group.

Rights Based Pathway Pilot

2.52 The principle of policing by consent is fundamental to Scotland's social fabric. Providing everyone with a fair, just and effective policing response is our moral responsibility and legal duty. It is an operational imperative to maintain and build the crucial bond of trust with our communities from which we draw our legitimacy.

2.53 The purpose of the Rights Based Pathway is to meet commitments in the Joint Strategy, Cyber Strategy, the Emerging Technologies Independent Advisory Group (ETIAG) recommendations and the Police Scotland and Scottish Police Authority Memorandum of Understanding (MOU), to support decision making and to maintain public trust and confidence in the organisation in respect of it adoption and use of technology.

2.54 With the introduction of new technology in mind, the Joint MOU states:

> *"The Joint MOU will apply to new and emerging areas of strategy, policy or practice, but the use of the Protocol should lead to the identification of broader, thematic, issues for policing meriting broader strategic discussion.* ***For example, Police Scotland may seek to introduce new technologies to protect citizens against the growing range of digital threats and risks. There is, however, the need for a wider, contextual, discussion about the appropriate balance of duties of policing in Scotland, alongside the safety and privacy expectations and rights of the public."***

2.55 The express need for this approach was borne out of the lessons learned from Police Scotland's initial introduction of Digital Triage Devices in 2020. This process identified the importance of evidencing a structured human rights and ethical approach, which maximised stakeholder and public engagement and consultation, prior to implementation.

2.56 Police Scotland completely understand the need to ensure public confidence and appropriate safeguards in utilising such technologies, however the challenge is to balance this against our statutory obligations in keeping the public safe, whilst making best use of available technologies to assist us in this mission. This has also been echoed by the SPA and are seeking to ensure that we have a balance of governance to introduce new technology. The Rights Based Pathway is therefore the mechanism for us to deliver against the terms of the MOU.

2.57 A new Data Ethics Triage process has been implemented that will assess all data related and data driven technology projects that go through Police Scotland's Change process. The triage process will identify where ethical challenges may lie, provide a pathway to enhanced internal and external scrutiny and provide advice to projects to ensure that data and data driven technology is used legally and ethically.

2.58 The Data Ethics Triage process is an integral part of the Rights Based Governance Pathway to ensure that Police Scotland can demonstrate a consistent and proportionate approach to assessing data ethics and public interest considerations.

2.59 There has been extensive engagement and support internally and externally throughout the development of this process and in keeping with Police Scotland's Values of Fairness, Integrity, Respect and Human Rights we believe that this model is a significant step forward in providing public reassurance on the police use of technology – which both keeps people safe, whilst upholding their rights.

2.60 The Rights Based Pathway is focused on the deployment of existing technology. This process currently does not exist and will be evaluated so that any lessons learned can be incorporated into future governance processes to ensure a robust rights based approach. The pilot of this pathway will not replace existing governance structures or change portfolio processes.

Child Abuse Image Database – Facial Matching (CAID FM)

2.61 In support of the pathway, CAID (Child Abuse Image Database) Facial Matching (FM) has been identified as the technology which will be used as a proof of concept for the Rights Based Pathway.

2.62 CAID is the Child Abuse Image Database and contributes to the fight against Online Child Sexual Abuse and Exploitation (OCSAE). It helps identify and safeguard victims, makes investigating Child Sexual Exploitation and Abuse faster and more effective and supports international effort to remove images from the internet.

2.63 Since 2014, Police Scotland have contributed to CAID through the upload of Indecent Images of Children (IIOC) and it now hosts millions of abuse images.

2.64 Based on 2022/23 Q2 performance statistics, 936 OCSAE crimes were recorded in Scotland, an increase of 6.4% on the five year mean. Police Scotland's detection rate for this period is 68.4%, an increase of 2.4% on the five year mean.

2.65 Certain types of OCSAE referrals originate from the US National Centre for Missing & Exploited Children (NCMEC) and are notified to Police Scotland via the National Crime Agency (NCA).

- 2015 - 2021, there has been a 511.2% increase in these referrals.
- 2019 – 2021 these referrals generated 2,498 National Online Child Abuse Protection (NOCAP) investigations.
- 75.8% of these were suspect NOCAP investigations.
- 24.2 % were Child at Risk (CAR) NOCAP investigations (often a child uploading imagery themselves where it is not clear if there is associated criminality such as grooming behaviour).

2.66 Despite other improvements around process and pro-activity in this area, the growing demand is having a significant effect on the workloads and welfare of our officers/staff.

2.67 As part of the continuous improvement of CAID, the Home Office has introduced the use of a 'Facial Matching' (FM) capability. In simplistic terms, FM within CAID is currently where an image of an individual is uploaded by a law enforcement agency (LEA), with the aim of identifying if that individual is present within that database.

2.68 The introduction of this capability brings about efficiencies in respect of taking less time to review images. A case with 10,000 images would typically take up to 3 days. Now, after matching images against CAID, a case of a similar size can be reviewed in an hour. This has helped shift the balance between reviewing images to identifying victims, with the overarching aim of safeguarding children.

2.69 Following a successful pilot in 2020, with the exception of Police Scotland all UK forces now using CAID FM. In addition to the number of operational benefits it has also sought to improve the wellbeing of the officers/staff engaged in its use.

2.70 In January 2022, in terms of Police Scotland's use of this capability, a data ethics triage was been completed (January 2022) and assessed as 'MEDIUM' with the requirement to clarify various aspect of the software with the Home Office and the developer, NEC. These have been subsequently addressed during a demonstration of the technology provided to a Police Scotland Senior Solicitor, PDWP staff and the Chief Data officer.

2.71 In April 2022, it was presented to the Independent Ethics Advisory Panel (IEAP) who were supportive of Police Scotland introducing this technology to protect children and identify offenders whilst supporting the welfare of our own staff.

2.72 In advance of its introduction, the use of CAID FM has been reviewed and approved at the PDWP Professional Reference Group meeting (January 2023) and through all of Police Scotland's governance, including the Senior Leadership Board (April 2023).

2.73 Police Scotland currently has the network and hardware infrastructure in place to support the use of CAID FM. The adoption of this technology will vastly improve our effectiveness in investigating OCSAE crimes, balanced against the public's right to privacy and will improve the wellbeing of our officers and staff working in this space.

BERLA

2.74 It also the intention of Police Scotland to introduce the use of software known as BERLA, to support the evaluation of the Rights Based Pathway.

2.75 BERLA will increase our capability to obtain information from motor vehicles as part of serious crime investigations. This has been subject to the data ethics triage process (March 2022) and assessed as 'MEDIUM' with a risk relating to data management, which is mitigated through BAU processes.

2.76 In terms of consultation, consideration was given to referring BERLA to a conventional Police Scotland Independent Ethics Advisory Panel (IEAP) however no ethical dilemma suitable for referral was been identified

2.77 A DPIA and EqHRIA have also been completed.

Next Steps

2.78 Members are requested to endorse the planned programme of work outlined in terms of the Policing in a Digital World Programme, the Rights Based Pathway and to acknowledge CAID FM and BERLA have been through the pathway and as a result Police Scotland wish to activate this technology.

2.79 Incorporating a rights based approach to policing, that balances privacy and protection is critical. Public, colleague and stakeholder engagement will enable us to understand this as we consider how we develop and implement technology to support policing in Scotland. A Rights Based Governance Pathway will ensure that Police Scotland can demonstrate a consistent and proportionate approach to assessing data ethics and public interest considerations.

2.80 CAID FM and BERLA having been subject to a respective data ethics triage assessment meet the criteria for assessment through the pathway and through their introduction into the organisation, will enable the service to test the pathway over the next 6 months, enable learning and review and ensure the most effective approach to the introduction/adoption of new technology going forward.

2.81 As outlined previously, the progress of the PDWP, the Rights Based Pathway and the introduction of CAID FM and BERLA has been approved by the organisation, through the respective internal governance structures.

2.82 A slide presentation overview of this report incorporating the PDWP, Rights Based Pathway, CAID FM and BERLA will accompany this report and be delivered at the meeting.

3. FINANCIAL IMPLICATIONS

3.1 There are significant financial implications in this report. A modular approach will be adopted by the programme to facilitate delivery within the available resources per financial year. This year, £4.3m has been allocated and the PDWP Programme expenditure has been approved by the Change Board.

3.2 Despite the current financial challenges in order to meet the ambition of the strategy, significant investment in our people, technology, estates, processes and structure is paramount.

4. PERSONNEL IMPLICATIONS

4.1 There are personnel implications in this report. Additional Programme resources are required to deliver next stages. Longer term, organisational change will be proposed in relation to structures required to enhance capabilities to prevent and deal more effectively with cyber dependant and enabled crimes.

5. LEGAL IMPLICATIONS

5.1 There are no legal implications in this report.

6. REPUTATIONAL IMPLICATIONS

6.1 There are reputational implications for Police Scotland if the improved capabilities and capacity are not delivered.

7. SOCIAL IMPLICATIONS

7.1 There are no social implications in this report.

8. COMMUNITY IMPACT

8.1 There are no community implications in this report.

9. EQUALITIES IMPLICATIONS

9.1 There are no equality implications in this report. All relevant documents will be completed in line with the formal investment governance process e.g. at Business Case stage. This will include a full consideration of Rights-based issues within relevant EQHRIA and DPIAs.

10. ENVIRONMENT IMPLICATIONS

10.1 There are no environmental implications in this report.

RECOMMENDATIONS

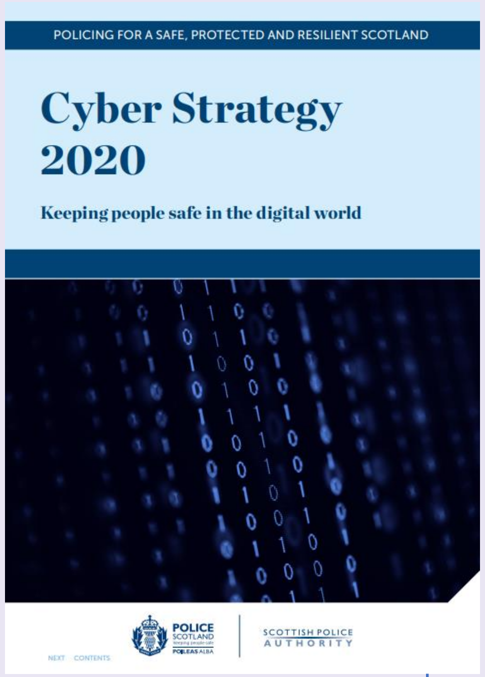
Members are invited to discuss the contents of this paper.

Policing in a [Digital World]

Programme Overview & Rights Based Pathway Pilot

SPA Policing Performance Committee 15 June 2023

ACC Andy Freeburn and CDIO Andrew Hendry



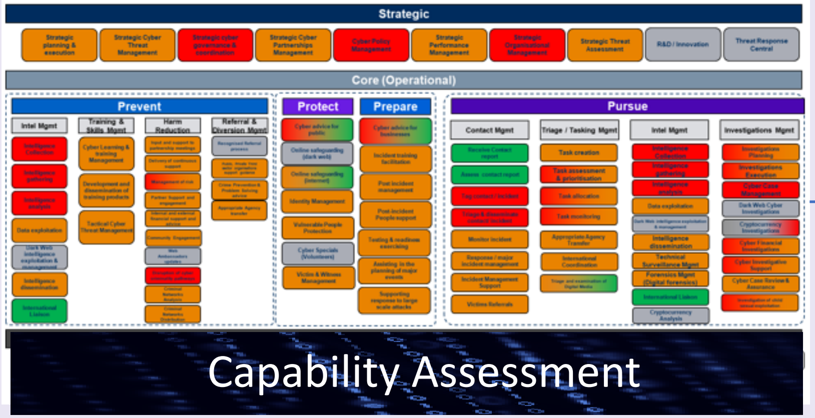
POLICING FOR A SAFE, PROTECTED AND RESILIENT SCOTLAND

Cyber Strategy 2020

Keeping people safe in the digital world

POLICE SCOTLAND | SCOTTISH POLICE AUTHORITY

NEXT CONTENTS



Strategic

- Strategic planning & execution
- Strategic Cyber Threat Management
- Strategic cyber governance & coordination
- Strategic Cyber Partnerships Management
- Cyber Policy Management
- Strategic Performance Management
- Strategic Organisational Management
- Strategic Threat Assessment
- R&D / Innovation
- Threat Response Central

Core (Operational)

Prevent

Intel Mgmt
- Intelligence Collection
- Intelligence gathering
- Intelligence analysis
- Data exploitation
- Dark Web intelligence exploitation & management
- Intelligence dissemination
- International Liaison

Training & Skills Mgmt
- Cyber Learning & training Management
- Development and dissemination of training products
- Tactical Cyber Threat Management

Harm Reduction
- Input and support to partnership meetings
- Delivery of continuous support
- Management of risk
- Partner Support and engagement
- Internal and external financial support and advice
- Community Engagement
- Web Ambassadors updates
- Disruption of cyber criminality pathways
- Criminal Networks Analysis
- Criminal Networks Distribution

Referral & Diversion Mgmt
- Recognised Referral process
- [illegible]
- Crime Prevention & Problem Solving advice
- Appropriate Agency transfer

Protect
- Cyber advice for public
- Online safeguarding (dark web)
- Online safeguarding (internet)
- Identity Management
- Vulnerable People Protection
- Cyber Specials (Volunteers)
- Victim & Witness Management

Prepare
- Cyber advice for businesses
- Incident training facilitation
- Post incident management
- Post-incident People support
- Testing & readiness exercising
- Assisting in the planning of major events
- Supporting response to large scale attacks

Pursue

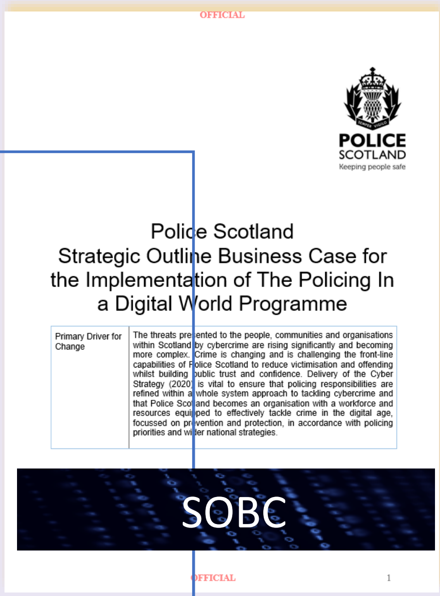
Contact Mgmt
- Receive Contact report
- Assess contact report
- Tag contact / incident
- Triage & disseminate contact/ incident
- Monitor incident
- Response / major incident management
- Incident Management Support
- Victims Referrals

Triage / Tasking Mgmt
- Task creation
- Task assessment & prioritisation
- Task allocation
- Task monitoring
- Appropriate Agency Transfer
- International Coordination
- Triage and examination of Digital Media

Intel Mgmt
- Intelligence Collection
- Intelligence gathering
- Intelligence analysis
- Data exploitation
- Dark Web intelligence exploitation & management
- Intelligence dissemination
- Technical Surveillance Mgmt
- Forensics Mgmt (Digital forensics)
- International Liaison
- Cryptocurrency Analysis

Investigations Mgmt
- Investigations Planning
- Investigations Execution
- Cyber Case Management
- Dark Web Cyber Investigations
- Cryptocurrency Investigations
- Cyber Financial Investigations
- Cyber Investigative Support
- Cyber Case Review & Assurance
- Investigation of child sexual exploitation

Capability Assessment



OFFICIAL

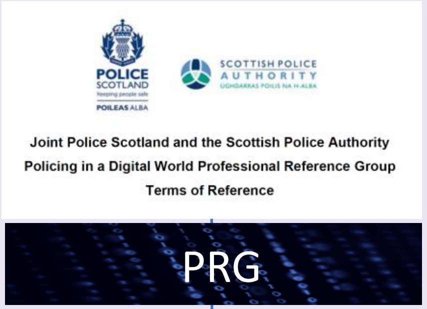
POLICE SCOTLAND
Keeping people safe

Police Scotland
Strategic Outline Business Case for
the Implementation of The Policing In
a Digital World Programme

Primary Driver for Change	The threats presented to the people, communities and organisations within Scotland by cybercrime are rising significantly and becoming more complex. Crime is changing and is challenging the front-line capabilities of Police Scotland to reduce victimisation and offending whilst building public trust and confidence. Delivery of the Cyber Strategy (2020) is vital to ensure that policing responsibilities are refined within a whole system approach to tackling cybercrime and that Police Scotland becomes an organisation with a workforce and resources equipped to effectively tackle crime in the digital age, focussed on prevention and protection, in accordance with policing priorities and wider national strategies.

SOBC

OFFICIAL 1



POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Joint Police Scotland and the Scottish Police Authority
Policing in a Digital World Professional Reference Group
Terms of Reference

PRG

Discovery

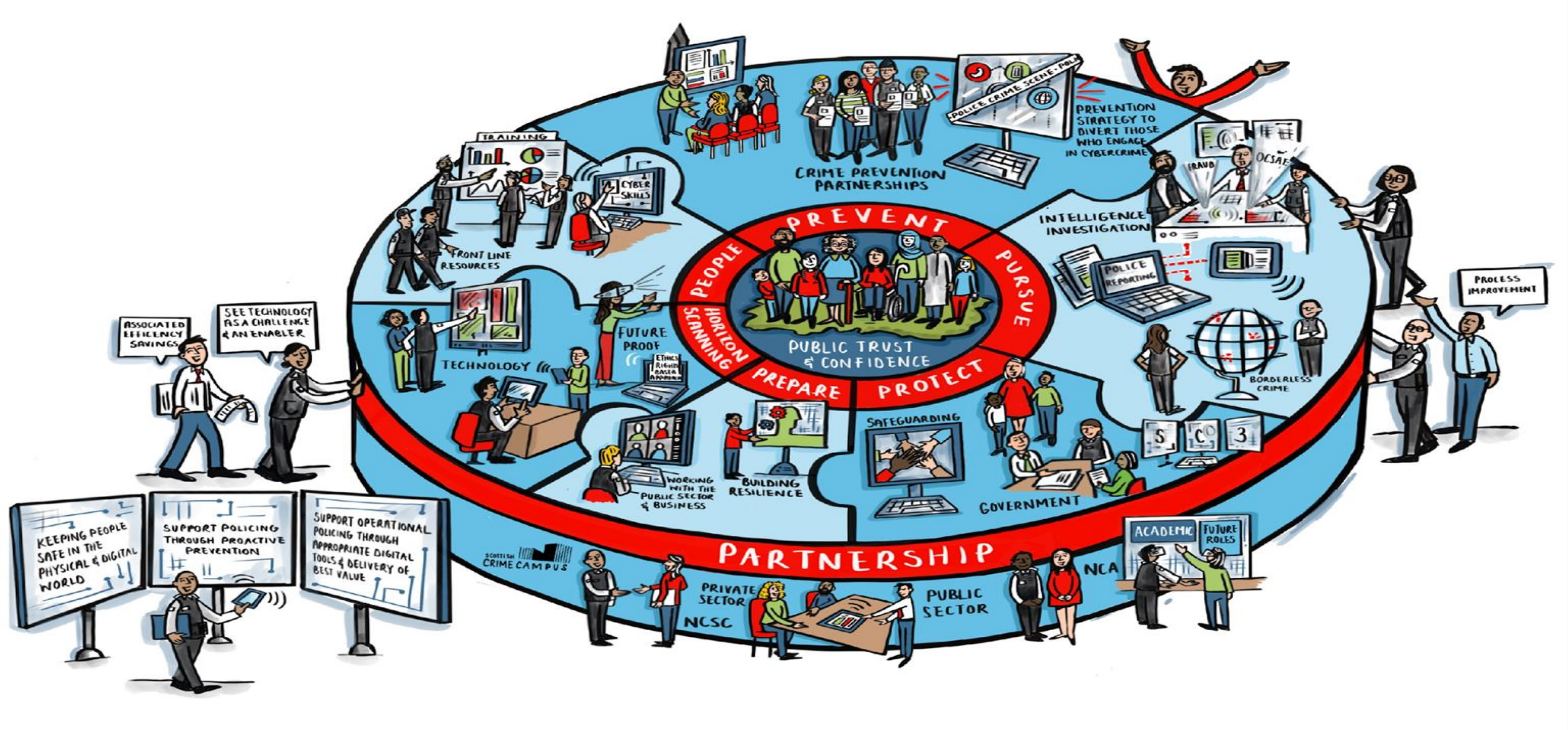
2020 2021 2022

Policing in a
[Digital World]

Drivers for Change

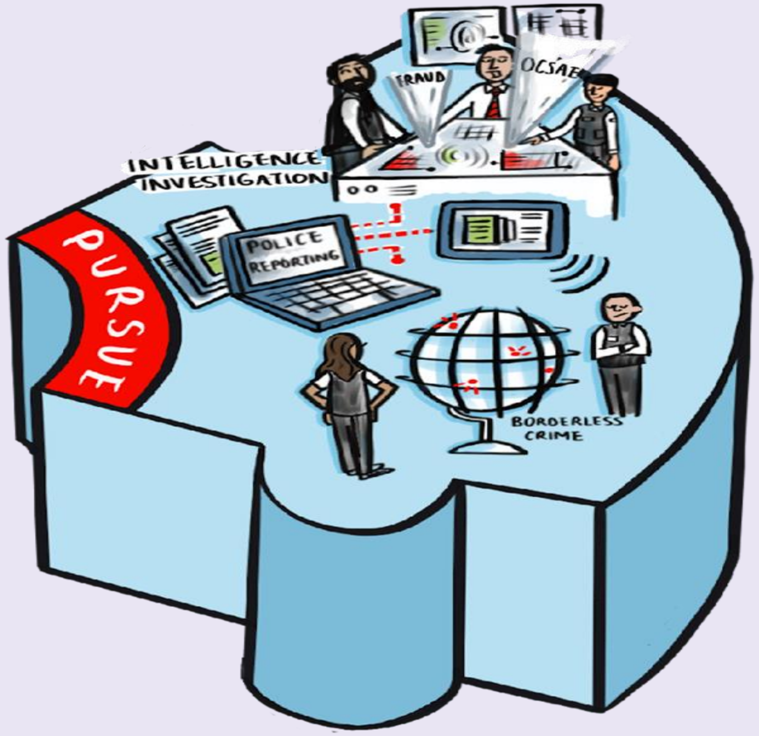
- Increase in Fraud - 68% over 5 years, 17% decrease in detection rates, 95% now online
- Increase in Online Child Sexual Abuse & Exploitation - 511% in last 5 years
- Digital Forensics Capability Improvements
- Specialist Cyber Capability Improvements

Target Operating Model


PREVENT
PURSUE
PROTECT
PREPARE
PEOPLE
HORIZON SCANNING
PUBLIC TRUST & CONFIDENCE
PARTNERSHIP
CRIME PREVENTION PARTNERSHIPS
POLICE CRIME SCENE
PREVENTION STRATEGY TO DIVERT THOSE WHO ENGAGE IN CYBERCRIME
FRAUD
OCSAE
INTELLIGENCE INVESTIGATION
POLICE REPORTING
BORDERLESS CRIME
PROCESS IMPROVEMENT
S C 3
SAFEGUARDING
GOVERNMENT
BUILDING RESILIENCE
WORKING WITH THE PUBLIC SECTOR & BUSINESS
ETHICS RIGHTS BASED APPROACH
FUTURE PROOF
TECHNOLOGY
FRONT LINE RESOURCES
TRAINING
CYBER SKILLS
ASSOCIATED EFFICENCY SAVINGS
SEE TECHNOLOGY AS A CHALLENGE & AN ENABLER
KEEPING PEOPLE SAFE IN THE PHYSICAL & DIGITAL WORLD
SUPPORT POLICING THROUGH PROACTIVE PREVENTION
SUPPORT OPERATIONAL POLICING THROUGH APPROPRIATE DIGITAL TOOLS & DELIVERY OF BEST VALUE
SCOTTISH CRIME CAMPUS
PRIVATE SECTOR
NCSC
PUBLIC SECTOR
NCA
ACADEMIC
FUTURE ROLES

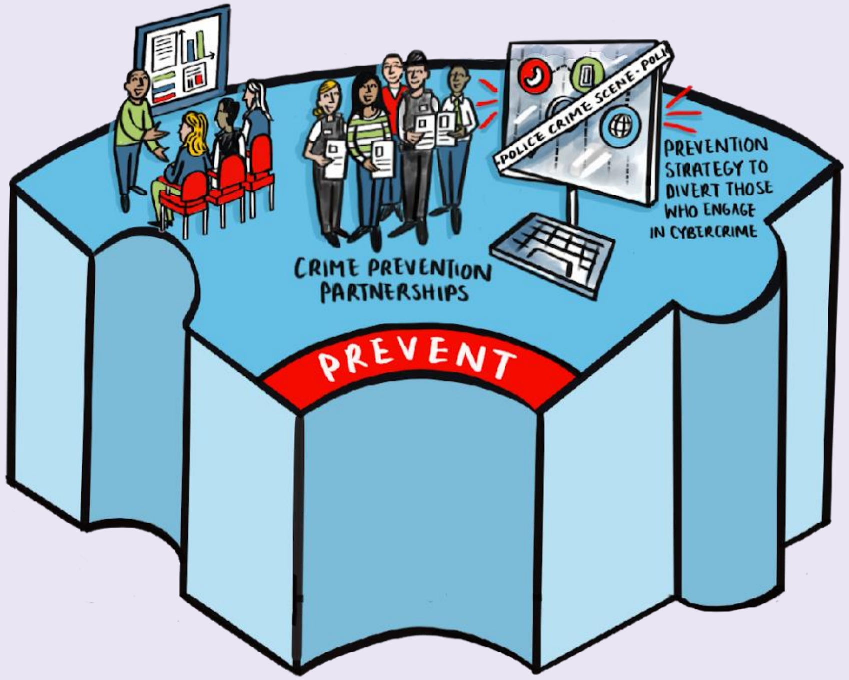
Tackling threats to public safety and wellbeing and keeping people safe in the physical and digital world.

Pursue - £4.3m investment this financial year



- Fraud
- Cyber Training & Capabilities
- Digital Forensics Capability Improvements
- Specialist Cyber Capability

Prevent


POLICE CRIME SCENE · POLI
PREVENTION STRATEGY TO DIVERT THOSE WHO ENGAGE IN CYBERCRIME
CRIME PREVENTION PARTNERSHIPS
PREVENT

- Cyber Harm Prevention
- Fraud Prevention

Partnerships

SCOTTISH CRIME CAMPUS
PARTNERSHIP
PRIVATE SECTOR
NCSC
PUBLIC SECTOR
NCA
ACADEMIC
FUTURE ROLES

- Multi Agency Fraud Hub
- Mapping Exercise
- National Police Chiefs Council
- National Crime Agency
- Cyber and Fraud Centre Scotland
- Cyber Scotland Partnership
- Scottish Cyber Coordination Centre
- Academia

POLICE SCOTLAND
POILEAS ALBA

Rights Based Pathway

The Balance of Rights When Introducing Technology for Policing in Scotland

Police Scotland/SPA Memorandum of Understanding (MOU)

"The Joint MOU will apply to new and emerging areas of strategy, policy or practice, but the use of the Protocol should lead to the identification of broader, thematic, issues for policing meriting broader strategic discussion. **For example, Police Scotland may seek to introduce new technologies to protect citizens against the growing range of digital threats and risks. There is, however, the need for a wider, contextual, discussion about the appropriate balance of duties of policing in Scotland, alongside the safety and privacy expectations and rights of the public."**

Introduction to Rights Based Pathway for Technology

- Development of Rights Based Pathway - To assess data ethics and public interest considerations when developing and implementing technology to support policing in Scotland.

- Consistent approach for both ‘New’ Technologies and for Enhancing ‘Existing’ Technologies, to ensure we prioritise privacy and protection.

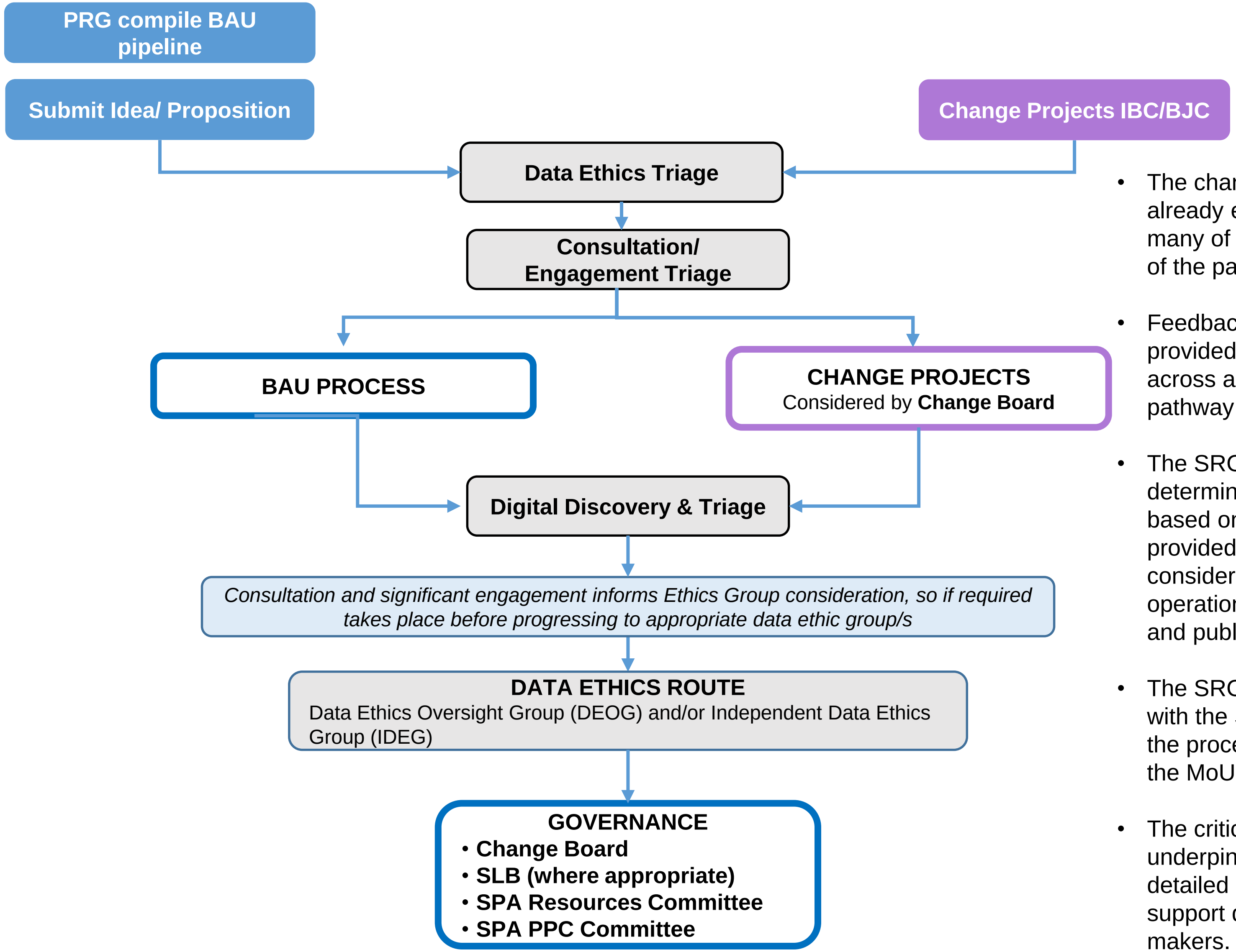
- Supports The Joint Strategy for Policing.

- Supports the Police Scotland/SPA MOU.

- Supports the ETIAG Recommendations.

- Activation of Child Abuse Image Database Facial Matching (CAID FM) to be used to test/evaluate the pathway.

Rights Based Pathway – Governance Process



Consultation and significant engagement informs Ethics Group consideration, so if required takes place before progressing to appropriate data ethic group/s

DATA ETHICS ROUTE

Data Ethics Oversight Group (DEOG) and/or Independent Data Ethics Group (IDEG)

GOVERNANCE

- **Change Board**
- **SLB (where appropriate)**
- **SPA Resources Committee**
- **SPA PPC Committee**

- The change process already encompasses many of the key areas of the pathway
- Feedback will be provided to the SRO across all stages of the pathway.
- The SRO will determine next steps based on advice provided and considerations such as operational imperative and public safety.
- The SRO will engage with the SPA through the process in line with the MoU.
- The critical pathway is underpinned by a more detailed process flow to support decision-makers.

Rights Based Pathway – Process / Engagement

Data Ethics Triage Process (11 Questions):

1. How large in scale is the project ?
2. Is it a major step change in capability?
3. Where does human decision-making sit within the outcomes of the project?
4. How novel is the project?
5. What kind(s) of data are to be used in the project, and for what purpose?
6. How would you categorise the quality and availability of the data required for the project?
7. Does the project involve data-sharing with other organisations?
8. How intrusive, punitive or coercive are the interventions which could result from the project?
9. To what degree could the project encroach on individuals' civil liberties, privacy or human rights?
10. Does the project involve objectives that have been subject of concern that suggest there might be problems with public acceptability of the project?
11. Is there reason to believe that the project will affect certain groups more than others, including groups with protected characteristics under the Equality Act?

Consultation & Engagement:

- Internal (Interdependencies)
- Data Ethics Oversight Group
- Independent Data Ethics Group
- Scottish Biometrics Commissioner
- Specific stakeholder engagement groups
- Scottish Police Authority (MOU)
- Professional Reference Group (PRG)
- Scottish Government
- Other Key Stakeholders
- NPCC
- Public
- Academia

Child Abuse Image Database (CAID) – Facial Matching (FM)

POLICE SCOTLAND
POILEAS ALBA

CAID is the Child Abuse Image Database and contributes to the fight against Online Child Sexual Abuse and Exploitation (OCSAE). As part of the continuous improvement, the Home Office has introduced the use of a 'Facial Matching' (FM) capability.

Governance

- **UK Pilot 2020** - With the exception of Police Scotland all UK forces now using CAID FM. It has been found to have a number of operational benefits and improves the wellbeing of the officers/staff engaged in its use.
- **DPIA/EqHRIA** - Produced by the PDWP for Police Scotland for the use of CAID FM.
- **January 2022** - Data ethics triage completed and assessed as 'MEDIUM' with the requirement to clarify various aspect of the software with the Home Office and the developer, NEC. These have been subsequently addressed during a demonstration of the technology provided to Police Scotland Senior Solicitor, PDWP staff and the Chief Data officer.
- **April 2022** - Presented to the Independent Ethics Advisory Panel (IEAP) who were supportive of Police Scotland's use of this technology to protect children and identify offenders whilst supporting the welfare of our own staff.
- **October 2022** – Consultation with the Scottish Biometrics Commissioner.
- **February 2023** – Endorsement at the Policing in a Digital World Programme Board and DCC Crime and Operations Management Board.
- **4 April 2023** - Endorsed at Change Board.
- **12 April 2023** - Approved by the Chief Constable at the Strategic Leadership Board.