SCOTTISH POLICE AUTHORITY

Agenda Item 5.2

Meeting	SPA Audit, Risk & Assurance Committee
Date	4 May 2022
Location	Via MS Teams
Title of Paper	Data Ethics Governance Framework
Presented By	ACC Alan Speirs - Professionalism & Assurance Denis Hamill - Chief Data Officer
Recommendation to Members	For Discussion
Appendix Attached	Yes Appendix A – Data Ethics Strategy Appendix B – Data Ethics Framework

PURPOSE

The purpose of this report is to summarise proposals to adopt a Data Ethics Strategy for Police Scotland and accompanying Data Ethics Governance Framework, which sets out how Police Scotland plans to meet its ambition to become "an organisation driven by effective and efficient use of data, in an ethical way."

The proposed data ethics strategy and governance framework will guide Police Scotland in the responsible use of data and data-driven technology, and provide the governance required to identify and address ethical challenges posed by novel uses of data and data-driven technology.

This is an enabling Framework, which will ensure a consistent approach to making decisions, whilst not constraining responsible innovation.

Members are invited to discuss the content of this paper.

1. BACKGROUND

1.1 Police Scotland aims to become "an organisation driven by effective and efficient use of data, in an ethical way." To achieve this, Police Scotland has developed a Data Ethics Strategy and Data Ethics Governance Framework in order to identify and address the ethical considerations posed by the use of data and data-driven technology.

1.2 Data provides new opportunities and the potential for innovation, but Police Scotland need to get this right by driving the responsible use of data. Data ethics is not about constraining this potential, but about the responsible and trustworthy use of data.

1.3 Many organisations across the public and private sector are seeking to make better use of data and emerging technologies to support decision-making. In line with this wider trend, police services are using, or considering developing, data-driven technology to derive insight and generate predictions to inform resource and operational decisions.

1.4 The NPCC divides data-driven technology in policing into 4 sub-categories: Artificial Intelligence and Algorithms, Biometrics, Digital Forensics, Surveillance and Investigatory Powers. Whilst there are different ownership, governance and legal frameworks for these sub-categories, from a policing and public perspective similar ethical considerations arise in how these technologies are designed, developed and deployed.

1.5 It is imperative that Police Scotland lead by example by setting the right foundations, processes and daily practices to use data and data-driven technology.

1.6 The Strategy and Framework have been developed in collaboration with the Centre for Data Ethics and Innovation (CDEI) and through engagement across the police service and externally, with academics, civil society and Scottish Government.

1.7 The Centre for Data Ethics and Innovation (CDEI) guides and supports organisations to maximise the benefits of data-driven technologies and enable trustworthy innovation. Formally a part of the UK Government's Department for Digital, Culture, Media and Sport, the CDEI provides support to a wide range of public and industry bodies, and is underpinned by an expert advisory committee of specialists who contribute their expertise to the CDEI's projects.

Their goal is to support partners in enabling and delivering responsible innovation in data-driven technology, creating an environment in which:

- the public are confident their values are reflected in the way data-driven technology is developed and deployed;
- we can trust that decisions informed by algorithms are fair; and
- the risks posed by innovation are identified and addressed.

The CDEI has worked with the policing sector over the last three years and has commissioned and published research on the use of technology in policing.

2. FURTHER DETAIL ON THE REPORT TOPIC

Approach to the Strategy

2.1 Police Scotland's approach to data ethics is principles-based and considers how these principles apply in the context of the decision being made. At the heart of policing in the UK is consent and legitimacy in the eyes of the public. Practically applying these principles should ensure that Police Scotland take a trustworthy approach to the use of data-driven technology as the service looks to innovate.

2.2 Underpinning this trustworthy approach must be a commitment to asking the right questions and developing robust, evidence-based and acceptable responses to them, which are open to internal and external scrutiny and challenge.

2.3 Guidance questions have been developed, structured by key themes, which are related to the responsible development and use of data and data-driven technology, including:

- **Value and impact**: The use of data and data-driven technology should provide value and benefit to individuals or society that is measured and evidenced.
- **Effectiveness and accuracy**: Data-driven technology in policing should be reliable and improve the accuracy of existing approaches. This should be monitored, audited and for particularly sensitive projects independently evaluated.

Good quality data is required to ensure the data-driven technology is reliable and effective.

- **Necessity and proportionality:** Any potential intrusion arising from police use of data must be necessary to achieve legitimate policing aims and proportionate in relation to the anticipated benefits.
- **Transparency and explainability**: The project's purpose, details of the data it uses, and notice of its deployment should be made public and open to scrutiny. Data-driven technology should be understood by relevant individuals using and affected by it.
- **Reliability and security:** Data-driven technology in policing should be reliable and measures should be in place to ensure data is used securely and protects privacy.

2.4 This approach to governance is designed to help Police Scotland identify potential harms, risks, and challenges and weigh these up with potential benefits and opportunities. Ultimately, being able to answer these questions should help Police Scotland deliver on their ambition to use data ethically.

Data Ethics Governance Framework

2.5 The Framework sets out how Police Scotland should govern its use of data and data-driven technology. It outlines robust mechanisms for internal input and challenge along with ways to invite independent advice. It also sets out practical guidance and repeatable processes for identifying the key ethical considerations when developing a data-driven project. If adopted, it will lay the groundwork for public confidence in Police Scotland's use of data.

2.6 The Framework recommends the governance required to identify and address ethical challenges posed by novel uses of data and data-driven technology. It is an enabling Framework, designed to ensure a consistent approach to making decisions and is not intended to constrain responsible innovation.

2.7 The Framework consists of two parts.

Part One sets out what good governance looks like for Police Scotland, including the internal and external mechanisms which will provide the expertise, challenge and advice needed.

Part Two offers practical guidance for Police Scotland to identify and address the key ethical challenges posed by the use of data and data-driven technology. It includes a toolkit which identifies key questions that Police Scotland should ask and answer, along the project lifecycle of a data-driven tool.

Triage of Risk – Data Ethics Risk Assessment

2.8 As the use of data and technology become more common, it can be challenging to determine whether a project is a data-driven project or project that simply involves data. Some projects are data-driven in a way that carries additional risk and requires additional governance.

2.9 To address this, the Data Ethics Governance Framework contains a set of eleven common triage questions to be used when considering a new project. Those projects which have been identified as carrying particularly high risk (as an outcome of the triage), will go through the detailed Framework process, thereby ensuring we focus only on those with the highest risk.

The triage questions consider a number of dimensions, including the scale and breadth of project, the data being used, the outcome/effects, and potential disproportionality. The detailed questions are found within the Framework

2.10 While the Triage questions were originally designed to carry out a risk assessment on projects, they could easily be applied to non-project initiatives and/or standalone decisions.

Alignment with the Memorandum of Understanding

2.11 Police Scotland and the Scottish Police Authority have recently formally agreed a Memorandum of Understanding (MoU) which aims to ensure early visibility and oversight of any new and emerging strategy, policy or practice under consideration by Police Scotland. The MoU will apply to all novel deployments and technologies. The Authority's main focus will be on significant equalities, human rights, privacy or ethical concerns raised, or where the issue will have a significant impact on public perceptions of, or confidence in, policing.

2.12 The aim is to provide early recognition of the public importance, a focus on understanding the public interest around it, and a shared critical pathway for assessment and anticipated outcomes. The MOU will use existing Police Scotland management controls and advisory mechanisms, and SPA governance systems, to achieve the aim.

2.13 It is proposed that the Data Ethics Triage process should be the mechanism to ensure that the goals of the MoU are implemented in a consistent and repeatable way. The Triage will be applied to all new projects, and can also be applied to any standalone operational initatives and/or decisions. The triage questions will evolve to meet the future needs of the MoU.

NPCC Alignment

2.14 Alongside our partnership, the CDEI is working with the National Police Chiefs' Council (NPCC), the Chief Scientific Advisor for National Policing and leads at individual forces, including West Midlands Police and the Metropolitan Police Service, to develop an Ethical Decision-making Guidance for the Use of Data Analytics in Policing. This builds directly on the Police Scotland Framework, but sets out a recommended national standard for how police forces should develop and use analytics.

2.15 The Guidance is likely to be circulated by the Chief Scientific Advisor for Policing and NPCC for written feedback to all UK forces and the intention is for it to then become the recommended national standard and possibly be turned into Authorised Professional Practice by the College of Policing.

Main Recommendations

2.18 Data and data-driven technologies have long been used to support Police Scotland's operations. However, data-driven technologies could be deployed in ways that might not be publicly acceptable. This calls for greater levels of scrutiny, oversight and transparency of particular uses of data and data-driven technology.

In particular, we recommend that Police Scotland:

1. **Data Ethics Triage** - Set up an internal Data Ethics Triage process, which would provide a data ethics risk assessment for all new project submissions, and also be used for relevant standalone operational initiatives/decisions.
2. **Internal Scrutiny** - Set up an internal Data-Driven Technology Oversight Group, which would provide internal support and

challenge for high-risk data-driven technology projects (as identified by the Triage process) throughout the project lifecycle.

3. **External Scrutiny** - Set up an external Independent Data Ethics Group, under the ownership of the Scottish Police Authority, to provide external review and advice to the SPA and Police Scotland senior leadership team on data-driven projects being proposed.
4. **Design Authority** - Accelerate the development of the internal Digital & Data Design Authority, with Data Design embedded in the scope. This would support, review and provide challenge at the 'Design' phase of a data-driven project.
5. **Alignment to Change process** - The guidance and controls laid out in the Data Ethics Governance Framework should be embedded into the BAU Change Governance process, and align with the existing PMO Stage Gates.
6. **Transparency** - Maximum transparency and engagement is encouraged and should be foundational to Police Scotland's use of data and data-driven technologies, both internally and externally. Whilst transparency in practice will necessarily look different across different use cases and the confines of the specific policing context need to be understood, in principle it should involve clear, comprehensive and accessible communications, tailored to the needs of different audiences. Where possible, transparency should be a proactive rather than a reactive process

3. FINANCIAL IMPLICATIONS

3.1 PSOS - One additional FTE (Data Ethics Lead) which is included within the CDO Target Operating Model project within the Data Drives Digital programme.

Annual revenue costs of approx. £54,000.

Julie MacLeod recruited as Data Ethics Lead and has been in post since February 2022.

4. PERSONNEL IMPLICATIONS

4.1 PSOS - One additional FTE (Data Ethics Lead) which is included within the CDO Target Operating Model project within the Data Drives Digital programme.

New role is part of the Chief Data Office, within Professionalism & Assurance.

5. LEGAL IMPLICATIONS

5.1 There are <u>no</u> further legal implications in this paper.

6. REPUTATIONAL IMPLICATIONS

6.1 There are <u>no</u> reputational implications associated with this paper.

7. SOCIAL IMPLICATIONS

7.1 There are <u>no</u> social implications associated with this paper.

8. COMMUNITY IMPACT

8.1 There are <u>no</u> community implications associated with this paper.

9. EQUALITIES IMPLICATIONS

9.1 There are <u>no</u> equality implications associated with this paper.

10. ENVIRONMENT IMPLICATIONS

10.1 There are <u>no</u> environmental implications associated with this paper.

RECOMMENDATIONS

Members are invited to discuss the contents of this paper.

DRAFT

Police Scotland: Draft Data Ethics Strategy

Purpose

The purpose of this Strategy is to set out how Police Scotland plans to meet its ambition to become "an organisation driven by effective and efficient use of data, in an ethical way."[1] The Strategy should be read alongside the Data Ethics Governance Framework which should help Police Scotland identify and address ethical considerations posed by data-driven technology. The Strategy and Framework should build confidence amongst internal stakeholders in Police Scotland and the Scottish public in how the service uses data-driven technology.

The Strategy, as with the Framework, has been developed in collaboration with the Centre for Data Ethics and Innovation (CDEI) and through engagement across the police service and externally, with academics, civil society and the Scottish Government. It draws on research the CDEI has conducted and commissioned looking at the use of algorithms in policing and wider research the CDEI has carried out on data sharing in the public sector. It also builds on intentions set out in Police Scotland's 2020 Strategy, in particular Strategic Outcome Three which states that the public, communities and partners are engaged, involved and have confidence in policing through embedding the ethical and privacy considerations that are integral to policing and protection into every aspect of the service and Strategic Outcome Five that Police Scotland is sustainable, adaptable and prepared for future challenges through using innovative approaches to accelerate our capability and capacity for effective service delivery.

Context

Data provides new opportunities and the potential for innovation, but Police Scotland need to get this right by driving the responsible use of data. Data ethics is not about constraining this potential, but about the responsible and trustworthy use of data.

Many organisations across the public and private sector are seeking to make better use of data and emerging technologies to support decision-making. In line with this wider trend, police services are using, or considering developing, data-driven technology to derive insight and generate predictions to inform resource and operational decisions. Data-driven technology in policing can be broadly subdivided into the following categories: Artificial Intelligence and Algorithms (used to provide back-office support and to assist operational decision-making), Biometrics, Digital Forensics, and Surveillance and Investigatory Powers. Whilst there are different ownership, governance and legal frameworks for these sub-categories, from a policing and public perspective similar ethical considerations arise in how these technologies are designed, developed and deployed.

Police Scotland is at an early stage in this journey. The service holds a wide range of datasets and draws on data to inform decision-making. Moreover, it deploys several data-driven tools for example to record information related to police vehicles, to optimise the deployment of officers, to detect if data is stored on a mobile phone and to take and store biometric data, including DNA and fingerprints. Some of the data-driven technology currently deployed is set out in more detail in Annex 1.

There has been significant progress in the service over the last five years in how the value of data is understood, along with the potential innovation it could bring. There is also a strong drive to set a high bar for using data and data-driven technology in a way that helps protect the Scottish public and is in line with the service's and wider policing principles and values.

[1] Joint Strategy for Policing 2020 'Policing for a safe, protected and resilient Scotland'; DDICT and Cyber Strategies

At a national level the Scottish Government has made its commitment to data ethics clear. Most recently, the government's Data and Intelligence Network developed a Data Ethics Framework which seeks to ensure ethical considerations are prioritised from the inception of a project and throughout, with access to the necessary input and independent oversight in place. At a UK level, whilst policing is a devolved matter, the National Police Chiefs' Council has set out an ambitious proposal for ensuring ethical accountability for how police use technology.

Given the wider national and UK context, Police Scotland want to lead by example by setting the right foundations, processes and daily practices to use data and data-driven technology.

Approach

Police Scotland's approach to data ethics is principles-based and considers how these principles apply in the context of the decision being made. The relevant policing and data principles are set out below and guide the service's decision-making around the use of data-driven technology. At the heart of policing in the UK is consent and legitimacy in the eyes of the public. Practically applying these principles should ensure that Police Scotland take a trustworthy approach to the use of data-driven technology as the service looks to innovate.

Underpinning this trustworthy approach must be a commitment to asking the right questions and developing robust, evidence-based and acceptable responses to them, which are open to internal and external scrutiny and challenge. This approach draws on the CDEI's Trust Matrix[2], which sets out key elements of a trustworthy approach enabling users to identify and address the key questions when starting a data-driven project in the public sector. These include:

- Value and impact: Who benefits and takes on risk from the data being used?
    - Is there a clear statement of the expected benefits of the use of data?
    - How are different groups (and individuals) in society affected?
- Accountability: Who is responsible for decisions about data use?
    - How are decisions made about acceptable levels of effectiveness and safety; the trade-offs between benefits and risks, including risks of privacy invasion or bias; levels of transparency and user control? Are the decisions and their rationale documented?
    - If individual subjects do not give explicit consent, what mechanisms are in place to ensure broader societal consent?
- Transparency: To what extent is the rationale and operation of the project open to public scrutiny?
    - Is an appropriate budget and resource in place to communicate the rationale for the project to those affected?
    - To what extent is the evidence of efficacy and privacy open to independent scrutiny through open source code and scientific evaluation?

This approach to governance is designed to help Police Scotland identify potential harms, risks, and challenges and weigh these up with potential benefits and opportunities. An approach to working through these questions, and others, is explored in more detail in the accompanying Governance Framework. Ultimately, being able to answer these questions should help Police Scotland deliver on their ambition to use data ethically.

[2] https://cdei.blog.gov.uk/2020/07/19/addressing-trust-in-public-sector-data-use/

Principles and values

The purpose of Police Scotland is to improve the safety and wellbeing of people, places and communities in Scotland, whilst our core focus is 'keeping people safe'.[3] Clear values and principles underpin how the service operates to achieve this. The Code of Ethics for Policing in Scotland sets out core values of fairness, integrity and respect, as well as the service's commitment to protecting human rights.[4] Upon attestation, new constables make a declaration to 'uphold fundamental human rights and accord equal respect to all people, according to law'.[5] All officers who previously took the police oath are now expected to understand the new declaration.

Meanwhile, the longstanding Peelian Principles, developed by Sir Robert Peel to define an ethical police service, established the approach of policing by consent and the importance of the police's legitimacy in the eyes of the public. The values at the core of the Peelian Principles, including integrity, transparency and accountability, continue to be as relevant today, in particular in light of the ethical considerations brought up by new technologies.

Such new technologies have driven Police Scotland to develop Data Principles[6], drawing on best practice from UK policing and the public sector more broadly. These principles are organised around six key areas:

1. Data as an asset: Data is recognised as an asset that has value to both Police Scotland and our partners and is critical to business decisions at all level
2. Data is accessible: Data will be accessible to everyone within Police Scotland, when and where they need it, unless there is a justification to withhold it
3. Data is trusted and fit for purpose: Data will be of a quality that is fit for its purpose, and linked to associated data sets, to enable operational and strategic policing benefits, and corporate services to drive value
4. Data is shared with partners: We will share relevant data with our partners, unless there is a justification to withhold it
5. Data is secure: Data will protected from unauthorised use and disclosure to ensure compliance with legislation and policing standards
6. Data use is ethical and compliant: Data will be used ethically and in compliance of legislations and national security.

This Strategy does not seek to define a new set of data ethics principles, but is underpinned by the existing policing and Data Principles Police Scotland has signed up to and drives their practical application in the context of policing in Scotland.

Benefits and opportunities

The effective use of data and data-driven technology has the potential to bring significant benefits to the police and citizens if developed and deployed ethically with a robust governance framework in place. Police Scotland have made a commitment in line with this, through their 2020 Strategy, to use the right tools and new technologies "in consultation with our people and the public" and with "strong and consistent ethical oversight that is open to scrutiny and maintains public trust." Police Scotland are also clear that we have an ethical obligation to use data available if it could help prevent harm,

[3] Scottish Police Authority (2020), Annual Police Plan 2020/21

[4] Police Scotland, The Code of Ethics for Policing in Scotland

[5] Scottish Parliament, Police and Fire Reform (Scotland) Act 2012. Section 10 https://www.legislation.gov.uk/asp/2012/8/section/10/enacted

[6] These Data Principles were presented and approved at a Police Scotland Data Governance Board meeting.

and therefore recognise the need to embrace new technologies and the opportunities they provide to enhance the effectiveness of policing.

Evidence is beginning to emerge around the efficiency gains which could be made through innovation in policing. Efficiency gains are being seen through time savings on more laborious bureaucratic tasks, such as manual data extraction, along with the more effective targeting of activity with less police resource. There is also potential for more efficiency gains in the future around the spotting of patterns of activity and potential crime, for example through the internet-of-things contributing a vast flow of information to police control rooms. Whilst it can be difficult for police forces to accurately measure the benefits of new technology due to the poor quality of baseline data available, as data collection, extraction and analysis becomes easier Police Scotland will be able to identify and assess these efficiency gains and wider benefits.

An example of the efficiency gains brought about through our investment in data-driven technology has been our use of Telematics, a data capture technology which manages its fleet of more than 3000 vehicles. Vehicle telematics uses a global positioning system (GPS) similar to a sat-nav device to monitor and record details about the vehicle, which are then fed back to a central management system. This system will be able to obtain data on the vehicle, driving performance and vehicle location. This data has multiple uses. It improves efficiency around vehicle maintenance and fuel consumption but wider than that it can be used if a road traffic collision occurs which enhances public trust through absolute transparency.

Risks and challenges

These opportunities and benefits need to be balanced and weighed up against the potential risks and challenges that data-driven technologies can bring about. For example, without sufficient care, processes could lead to outcomes that are biased against particular groups, or systematically unfair in other regards. And where these algorithmic tools are shown to be effective, they should only be assisting human decisions as AI is at its most beneficial when it is combined with human expertise allowing professional judgement and discretion. Where appropriate care has been taken internally to consider these issues fully, it is still critical for public trust in policing that Police Scotland is transparent in how such tools are being used.

There is a risk that tools are deployed with insufficient, unreliable or outdated data behind them. Without proper training of the users or rigorous evaluation, these tools could be opinion-based rather than evidence-based, and that they could override police officers unduly or are applied inconsistently. For example, there is a risk that a tool could be designed and deployed in such a way that it leaves the officer with little to no discretion.

Concerns have also been raised over the use of sensitive data to develop data analytics tools, in particular risks of indirect racial or gender bias in predictive tools. Even when models do not include a variable for race, postcode can function as a proxy variable for race or community deprivation in some areas, thereby having an indirect and undue influence on the outcome prediction. There are also particular risks with predictive models which target individuals, for example to understand their likelihood of reoffending, such as a high rate of false positive identifications and the consequences for that individual's personal privacy and liberty if they were to reoffend.

The use of data analytics tools may also undermine public confidence in policing. Recent research[7] by the Royal Society of Arts (RSA) and DeepMind highlights that people feel especially strong about the

[7] RSA - Artificial Intelligence: Real Public Engagement - https://www.thersa.org/globalassets/pdfs/reports/rsa_artificial-intelligence---real-public-engagement.pdf

use of automated decision systems in the criminal justice system (60 percent of people oppose or strongly oppose its use in this domain). Moreover, people are least familiar with the use of automated decision systems in the criminal justice system – 83 percent were either not very familiar or not at all familiar with its use. These findings show that there is a significant risk that if police forces move too quickly in developing these tools, without engaging and responding to public concerns and expectations, there could be significant public backlash and a loss of trust in the Police Scotland's use of data.

The use of data analytics tools in policing is likely to grow in both scale and sophistication in the coming years. Ethical and effective use of data and technology, undertaken in a way that engages and involves the public, can build public confidence in the service's use of data driven technology and in turn enable greater use of this technology for public benefit. However, if it is seen to be used secretly and without transparency the public may not trust it, even if it is proven to be effective.

Police Scotland are committed to addressing these challenges through implementing this strategy and the Governance Framework to ensure all decisions around the use of data-driven technology focus on ensuring public legitimacy and consent.

Operationalising the Strategy

In order to operationalise this strategy Police Scotland has developed a Governance Framework in order to identify and address the ethical considerations posed by data-driven technology and guide the responsible use of data-driven technology now and into the future. The Framework should help guard against misuse and potential harms, and build public confidence in Police Scotland as a data-driven organisation. It is an enabling Framework designed to help and guide Police Scotland in making decisions about the use of data-driven technology. It is not intended to constrain responsible innovation or add unnecessary layers of governance and bureaucracy. It is also key to Police Scotland adopting a sustainable approach to the use of data-driven technology driven by measured, strategic and open decision-making with delivering the policing purpose at its core.

Annex 1: Data use cases

Police Scotland's operations rely on the use of data. From frontline policing, where officers must collect comprehensive data pertaining to individual incidents, through to complex and long-term investigations which rely on the effective retrieval, organisation and analysis of multiple disparate data sources, policing is a data-driven endeavour. In recent years, Police Scotland has embarked on several specialist data initiatives, which form helpful use cases for the Strategy and Framework. These include:

- **Cyber Kiosks**: Desktop computers containing specialist software, enabling trained police officers to view information stored on a mobile phone or tablet, which may be relevant to a police investigation or incident. The planned rollout of Cyber Kiosks in 2019 was delayed, with the Scottish Parliament's Justice Sub-Committee on Policing requesting further information on the legal framework for their use. Cyber Kiosks were finally deployed in early 2020. As a data use case, Cyber Kiosks highlight challenges including public perception and communication, and due diligence processes prior to launch. It also is an example which may impact on future uses of tech/ data by Police Scotland given how high profile it has been.
- **Telematics**: 'Black box' devices installed in police cars to monitor factors such as fuel consumption, speed and drive behaviour. This data may be used to inform training, resourcing, vehicle procurement, and as a tool for management to improve efficiency but the

data collected tracks the movement of the entire fleet and adds a layer of transparency building greater public trust. Similar to Cyber Kiosks, the roll out of Telematics was delayed due to a lack of consultation and due diligence and as such, many of the 'tools' the system had to offer have been disabled.

- **Biometrics**: Police Scotland collects DNA, fingerprints and images from arrested persons for each arrest. A new Biometrics group is potentially going to be set up to focus on ethical questions around the use and retention of biometric data in Police Scotland. Ethical considerations around how long biometric data is retained by Police Scotland (following a recent EU ruling related to a case in the Police Service of Northern Ireland) have been discussed at the Independent Ethics Advisory Panel.
- **AI and Algorithms:** Police Scotland does not currently deploy any AI or algorithmic tools. However, it is currently partnering with the Scottish Government as part of The CivTech Alliance on a project to develop an explainable AI model. The specific use case Police Scotland has proposed is designing and building an automated system capable of processing multiple unstructured data sources coming from logs and notes using a natural language processing algorithm. Police Scotland is currently reviewing proposals from technology providers and building a test dataset for the successful provider to build the model on.

DRAFT

POLICE SCOTLAND
POILEAS ALBA

SCOTTISH POLICE AUTHORITY

Policing in Scotland: Data Ethics Governance Framework

Version: 1.2

Date: 13/04/2022

Version Number	Date	Comments
1.0	03/08/2021	
1.1	10/03/2022	Updates following engagement with SPA and conclusion of Data Ethics Triage pilot
1.2	13/04/2022	Updates following internal review within Police Scotland Chief Data Office

Executive Summary

This Framework sets out how the policing system in Scotland should govern its use of data and the development and deployment of data-driven technology. It recommends establishing robust mechanisms for internal input and challenge along with ways to invite independent advice. It also sets out practical guidance and repeatable processes for identifying the key ethical considerations when developing a data-driven project. The framework lays the groundwork for ensuring the public have confidence in the policing system in Scotland's use of data to keep them safe.

Introduction

Background

Police Scotland aims to become "an organisation driven by effective and efficient use of data, in an ethical way."[1] To achieve this, Police Scotland has developed[2] a Data Ethics Strategy and Data Ethics Governance Framework (Framework) in order to identify and address the ethical considerations posed by the use of data and data-driven technology.

The Framework is a living document which will be tested on specific use cases as Police Scotland explores ways to incorporate data-driven approaches and tools into its operations. Proactively embedding the Framework will be crucial in order to realise the benefits and value of technology. It also provides an opportunity for Police Scotland to share lessons with other police forces at the National Police Chiefs' Council.

Although developed by Police Scotland, the Data Ethics Governance Framework is also suitable for use by the Scottish Police Authority (Forensics) and adherence to the Data Ethics Framework will be a requirement for all projects engaged in the Police Scotland Change process.

The Framework compliments the Memorandum of Understanding (MOU) signed by the Chief Constable of Police Scotland and the Chair of the Scottish Police Authority in 2021 on engagement and communication relating to new and emerging strategy, policy or practice in areas of significant public interest.

Aims

The purpose of this Framework is to guide those responsible for policing in Scotland in the responsible use of data and data-driven technology now and into the future. The Framework recommends the governance required to identify and address ethical challenges posed by novel uses of data and data-driven technology. It is an enabling Framework, designed to ensure a consistent approach to making decisions and is not intended to constrain responsible innovation. It should help both highlight where data may be being underused, through an emphasis on identifying problems and controlled testing

[1] Police Scotland's 'Policing 2026' strategy

[2] The Framework, as with the Strategy, has been developed in collaboration with the Centre for Data Ethics and Innovation (CDEI) and through engagement across the police service and externally, with academics, civil society and the Scottish Government. It draws on research the CDEI has conducted and commissioned looking at the use of algorithms in policing and wider research the CDEI has carried out on data sharing in the public sector. It also builds on intentions set out in Police Scotland's 2026 Strategy and the approach to addressing ethical considerations in the Scottish Government's Data Ethics Framework.

and experimentation, but also guard against the misuse of data and potential harms. Its use should also build public confidence in Police Scotland and the SPA as trustworthy stewards of data.

Approach

The Framework consists of two parts. Part One sets out what good governance looks like, including the internal and external mechanisms which will provide the expertise, challenge and advice needed. Whilst existing bodies, structures and processes will be drawn on for decisions around policing strategies, priorities and operations, the Framework recommends what is needed in addition to address the thornier ethical challenges that may arise through the use of data and data-driven technology in the future.

Part Two offers practical guidance to identify and address the key ethical challenges posed by the use of data and data-driven technology. First, it sets out a triage approach for to categorise data-driven technology projects according to levels of ethical risk. This triage approach may also be used in future for Police Scotland to run a risk assessment on operational decisions.

Next, Part Two identifies key questions that the policing system in Scotland should ask and answer, along the lifecycle of those data-driven technology projects with higher levels of ethical risk. These questions are not intended to be read or used as a check-list, but instead as prompts for project teams to consider and for senior leaders and oversight bodies to probe when reviewing new project proposals.

By providing responses and actions to these questions and logging these, the policing system in Scotland will be able to document and learn from its decision-making. Moreover, if the responses and actions are robust and evidence-based this should build public confidence that those responsible for policing in Scotland are carefully considering and addressing the key ethical considerations and provide assurance to regulators and oversight bodies.

Scope and terms

For Police Scotland, an ethical approach is about “doing the right thing, in the right way”.[3] In the context of data and data-driven technology, it is also about acting in a trustworthy way through the responsible procurement, development, deployment of such technology.

‘Data-driven technology’ is used in the Strategy and Framework as a deliberately broad term to encapsulate:

- information processing and analytics applied to data and
- technologies which are either dependent and based on the availability of data, or which generate new data, and
- new or emerging technologies.

The National Police Chief’s Council divides data-driven technology in policing into four key sub-categories[4]: Biometrics, Cyber and Digital Forensics, Surveillance and Investigatory Powers, and Artificial Intelligence (AI) and Algorithms.

[3] As set out in the ToRs for Police Scotland’s Independent Ethics Advisory Panels

[4] These are the sub-categories in the NPCC Digital Ethics Strategy.

Whilst there are different governance and legal frameworks for these sub-categories, from a policing and public perspective similar ethical considerations arise in how these technologies are designed, developed and deployed. This Framework should be used by Police Scotland and SPA Forensics to identify and address the ethical considerations that may arise through data-driven technologies across all four sub-categories, with the exception of covert surveillance and Investigatory Powers (IP) Act capabilities[5] which are out of scope bearing in mind the specific legal framework governing their use. Annex 1 sets out how these sub-categories are defined, along with current Police Scotland use of data-driven technology in these areas and potential future use cases.

This Framework applies to projects which use data or data-driven technology. The lifecycle in Part Two is designed to apply specifically to projects with higher levels of ethical risk, such as those which are particularly large in scale, particularly complex in terms of data-sharing, which involve controversial objectives or which the public may be less likely to find acceptable. The triage process in Part Two is designed to identify such projects; however, the triage process itself may still be useful in analysing lower risk projects, and identifying particular issues which require further investigation.

As the Framework is operationalised, the criteria for higher risk projects within the triage process will be tested and refined. In other words, the Framework is intended to be an evolving document.

Audience

The Framework is primarily intended for those Police Scotland officers and staff and SPA Forensics staff who are responsible for developing, implementing, working with or approving the use of data or data driven technology. It should also be useful for Police Scotland and SPA Forensics personnel working with external data scientists (private sector contractors, project management consultants, data scientists or academics).

Police Scotland’s Chief Data Office will be responsible for conducting the Data Ethics Triages described later in this document for all Police Scotland projects and those SPA Forensics projects managed by Police Scotland’s PMO. The Chief Data Office will also have overall responsibility on behalf of the policing system in Scotland for the ongoing review of the Data Ethics Framework.

The Framework also supports existing internal and external governance bodies such as Police Scotland’s Ethics Advisory Panels, the Scottish Police Authority, the Information Commissioners’ Office, and the Scottish Government, in holding Police Scotland and SPA Forensics to account for their use of data-driven technology.

Recommendations

Mechanisms for internal advice and external scrutiny

Data and data-driven technologies have long been used to support the policing system in Scotland’s operations.

However, data-driven technologies could be deployed in ways that might not be publicly acceptable.

[5] This Framework does not cover covert surveillance or investigatory powers. These raise an additional set of questions around necessity and proportionality of intrusion, collateral intrusion, classification of data which are not covered here and are governed by either the Investigatory Powers Act 2016 (IPA), the Regulation of Investigatory Powers (Scotland) Act 2000 or the Regulation of Investigatory Powers Act 2000 (RIPA)

This calls for greater levels of scrutiny, oversight and transparency of particular uses of data and data-driven technology. In particular, Police Scotland as the lead on the implementation of this Framework should:

1. Implement the **data ethics triage process** set out in Part Two of this Framework. This process can be applied to all new projects and in future to standalone operational decisions/ initiatives, assessing the relevant level of ethical risk.

2. Accelerate the development of the internal **Digital and Data Design Authority** (with data in scope). This Authority should support, review and provide challenge at the 'Design' phase of a data-driven project.

3. Set up an internal **Data-Driven Technology Oversight Group**, which would provide internal support and challenge for algorithmic or AI projects throughout the project lifecycle.

4. Set up an external **Independent Data Ethics Group**, under the banner of the Scottish Police Authority, to provide external review and advice to the SPA Chief and Police Scotland / SPA Forensics senior leadership on data-driven projects being proposed.

The rationale, roles and responsibilities of these bodies are set out in more detail in Part One. In setting up these bodies, Police Scotland should ensure they are properly supported by relevant officers and staff and there are clear feedback loops to project teams and decision-makers to ensure advice properly feeds into the development of new projects. Whilst these bodies should bolster expertise and scrutiny, Police Scotland (and its Chief Constable) and / or SPA Forensics (and its Director) will remain ultimately responsible and accountable for their use of data and data-driven technology.

Transparency

Maximum transparency and engagement is encouraged and should be foundational to the use of data and data-driven technologies, both internally and externally. Whilst transparency in practice will necessarily look different across different use cases and the confines of the specific policing context need to be understood, in principle it should involve clear, comprehensive and accessible communications, tailored to the needs of different audiences. Where possible, transparency should be a proactive rather than a reactive process.

Identifying and addressing ethical considerations

Those responsible for policing in Scotland should follow and build on the guidance set out in Part 2 in order to identify and address the key ethical considerations that could arise from the use of data and data driven technology.

Part One: Governance of data and data-driven technology

Good governance

Clear, robust governance is needed to ensure that data and data-driven technologies are used in responsible ways. This should be established before significant steps are taken to invest in new technologies so as not to risk undermining public confidence.

In the context of a responsible approach to the use of data and technology in policing in Scotland, good governance means:

- **Establishing robust mechanisms** for internal input and challenge, and external advice, on decision-making. This should include ensuring that risks and harms are properly understood and weighed up.

- **Establishing clear responsibility and accountability** for new uses of data and data-driven technology. This should include identifying the key decision-makers and decision points along the project lifecycle, within the existing policing chain of command.

- **Putting in place repeatable processes** to identify, address and test ethical considerations and ensure consistency of approach and auditability.

The approach to good governance in this Framework will also drive other benefits which will overall contribute to building confidence in Police Scotland and SPA Forensics as trusted stewards of data.

Embedding the Framework will help raise the bar in the following ways:

- **Being transparent and open** about the use of data and data-driven technologies, communicating such uses clearly, accessibly and, where possible, proactively.

- **Engaging with diverse views** and collecting input on the uses of data and data-driven technologies and, where appropriate, demonstrating the path to impact such engagement has.

- Drawing, and building on, **specialist and multi-disciplinary expertise** to ensure the use of data and data-driven technology is robust, evidence-based and effective.

- Clearly **articulating the purpose and value** of the use of data and data-driven technologies and ensuring these are measured and met. This should include identifying the trade-offs and considering what is publicly acceptable.

- **Identifying and mitigating potential harms** that may arise from novel uses of data.

- Creating an **environment for responsible innovation**, whereby new approaches can be explored within frameworks of rigorous oversight, evaluation and transparency.

DRAFT

The section below sets out the internal and external bodies Police Scotland should set up and how these should work alongside existing bodies to ensure the appropriate governance of data-driven technologies.

Internal

This Framework recommends Police Scotland set up the following internal bodies to ensure appropriate governance.

Data-driven Technology Oversight Group

This will be a 'project level', advisory group involved throughout the lifecycle of a project. It will provide input, oversight and challenge specifically on proposed data-driven projects[6]. The Group will be chaired by the Chief Data Officer and membership will include the Head of Information Assurance and Data Ethics, the Data Ethics Lead, internal Police Scotland data analysts, data scientists, Police Scotland's Data Protection Officer, representatives from Information Assurance, a legal advisor, representatives from SPA Forensics and leads in the Professional Standards Unit.

The Data-driven Technology Oversight Group will provide a centralised place for Police Scotland and SPA Forensics to draw on and invest in specialist expertise in data science and data analysis, improving its ability to develop and test new data-driven tools and building an evidence base of what works. The Group will also provide a forum for discussion about the legal, data protection and equality considerations of new data-driven tools.

The Data-driven Technology Oversight Group may also look to bring in external expertise on an ad-hoc basis to ensure it is drawing on the latest academic research and best technical expertise available. The Group could bring in data scientists and academics with expertise in police use of data and technologies at universities and research institutes. Formal partnerships, with secure data sharing arrangements, to design and test new models should be explored, along with arrangements to allow for the independent evaluation of the models Police Scotland and the SPA deploy.

In order to ensure a high bar for transparency, the Data-driven Technology Oversight Group should be responsible for maintaining and updating a public register of data-driven technologies which have the potential to impact the public[7].

This should include both proposed and live projects. There may be cases where the disclosure of particular information about a technology could undermine operational capability, for example with regards to covert or IP Act capabilities (which we have specified fall out of scope for this Framework). However, the Data-driven Technology Oversight Group should push for maximum transparency and, in these cases, either publish the rationale for including certain capabilities in their register or provide a very high level description of the relevant technology.

The Group should also drive Police Scotland to issue proactive communications regarding time and place-specific deployments, along with publishing details of trials of new technologies, their results and next steps. The Group could also find creative ways of publishing new data or data insights generated by data-driven tools in accessible formats. All of this should be done whilst recognising the policing context and without compromising live or ongoing operations.

[6] AI is an umbrella term for a range of technologies aimed at replicating human intelligence abilities in digital computers. AI refers mainly to systems that use machine learning for pattern detection, prediction, human-machine dialog, and robotic control. An algorithm can be understood as a set of precise instructions that describe how to process data, typically in order to perform a calculation or solve a problem.

[7] It is likely that the projects published in a register would also fall under the scope of an FOI(S)A request.

Digital and Data Design Authority

The Digital and Data Design Authority has previously been proposed by the Strategic Design Authority. The Authority will be an advisory group, responsible for supporting and reviewing ideas for data-driven projects at the 'Design' stage of a project, and providing a foundation for responsible innovation. It will provide an internal forum for experimentation and testing in a controlled environment.

Existing internal groups

These groups will work alongside the relevant governance bodies that already exist including the Change Board, Data Governance Board, the Strategic Design Authority and groups like the Cyber Resilience and Digital Capability Board and Biometrics Oversight Board.

Data-specific ethical challenges may also be discussed at the internal national and regional ethics advisory panels Police Scotland has in place. For example, these panels could be used by police officers and staff in Police Scotland to seek advice on whether they should explore a new use of data or data-driven technology.

External

External advice and challenge is essential to Police Scotland / SPA Forensics using data in a trustworthy way. As Police Scotland and SPA Forensics look to innovate more, enabling independent, expert challenge of the design, development and deployment of data-driven projects will be crucial for securing public confidence. This Framework recommends the establishment of an Independent Data Ethics Group[8].

Independent Data Ethics Group

The Group should be advisory, not a decision-making body, however the advice should be sought before decisions are made.

The Group's **function and ways of working** will need to be carefully considered. It will need to operate independently with the right structures in place to support and enable it to be challenging and effective. Suggestions as to how this could be done include:

- Set up the Group under the Scottish Police Authority (SPA) and run it from the SPA's Office, whilst ensuring the buy-in of the Chief Constable and SPA Forensics Director.
- Set up the Group with a clear purpose i.e. to advise the Chair of the SPA, Chief Constable and SPA Forensics Director on data-driven projects being proposed by Police Scotland, before significant decisions are made.
- Create an organisational culture that regards the Group as an essential part of delivering a successful project rather than a burden or a constraint.
- Ensure the attendance of the relevant operational lead for the project being discussed at the Group meeting.
- Ensure the Group maintains confidentiality of the projects discussed.

[8] A small number of forces in England and Wales (West Midlands Police and Essex Police) have set up an Independent Data Ethics Committee. Whilst a standard terms of reference for individual police force committees does not currently exist, lessons can be drawn on from the experiences of existing Committees in policing and the public sector more widely for how this group could be set up.

- Ensure the Group has rights to information related to the projects discussed in order to be able to give informed advice.
- Refrain from giving public assurances about an ethical approach by purely highlighting the establishment of an ethics Group. This risks undermining the trust of members who may feel they are simply being used to fulfil a presentation or communications requirement rather than providing constructive challenge. Instead, put in place clear, robust transparency measures including a publicly-available summary of Group discussions and decisions.
- Agree a way in which the Group will provide its outputs and advice i.e. choosing from a range of options including ‘Proceed with project with no amendments’, ‘Proceed with project with minor amendments’, ‘Rejects project’.
- Minutes of Group discussions should be published. These should follow best practice accessibility requirements.

Police Scotland and SPA Forensics will need to consider whether the Group publishes its advice. In publishing the advice, Police Scotland and SPA Forensics may find it difficult not to follow it and make them feel like they are seeking permission, rather than challenge, from the Group. This, in turn, could risk them losing some responsibility over decision-making. Publishing the advice may also impact how frank and direct the Group feels like they can be, especially if they would then need to justify it in a public domain.

On the other hand, publishing the advice would be one way to give the Group teeth and to ensure those responsible for policing in Scotland have to listen and give a clear rationale if they were to contravene the Group’s recommendation.

When agreeing the **membership** of the Group, careful thought must be given to the function members are expected to perform. This must be understood and agreed by members in order to facilitate constructive discussions and enable the Board to fulfil its role. Suggestions for how to ensure the right membership include:

- Be guided by the stated purpose and role of the Group when recruiting the members.
- Ensure the expertise of members combines academic, legal, data science and ethics expertise so that the Group can provide the necessary advice and challenge. Ensure the Group members have the expertise to interrogate the scientific robustness and effectiveness of the project being proposed.
- Take time and invest in following best practice in diversity and inclusion when recruiting members and ensure representation from individuals with strong links to the community. Diversity in membership is important for broader representation and establishing public trust.
- Ensure time commitments from members are clear from the outset. If possible, remunerate members for their time.
- Encourage mechanisms for the Group to engage more widely and seek additional expertise and views if necessary i.e. hearing from individuals with relevant lived experience.

Separate to the Group, Police Scotland and the SPA’s use of data and data-driven technology falls under a wider network of external oversight, which includes some of the bodies and organisations set out in Annex 2.

Governance in practice

In order to operationalise this Framework, it is recommended that Police Scotland and SPA Forensics agree a standard process for any new use of data or data-driven technology. The Agile project delivery cycle (referred to here as the project lifecycle), as defined in the UK government's service manual[9], provides a useful framework for overall project management of police data-driven projects[10]. We have used the Agile project delivery cycle as a basis for the Guidance in Part Two, but have made some amendments to best suit policing in Scotland's needs. These amendments include:

- Separating out the Discovery phase into Problem Identification and Design to allow for a focused discussion of new ideas and problems which could be addressed through a data-driven technology and an opportunity to consult the relevant Ethics Advisory Panel where relevant. This should also ensure senior leaders and decision-makers are able to interrogate whether a problem is best suited to a data-driven approach. It makes transparent that there are well defined decision points and appropriate criteria for authorising research into the potential of data driven approaches and authorising the deployment of such systems. Renaming the stages so they are more easily understood by a wider, non-technical, audience.
- Tailored the description of the stages to suit the policing context.
- Added questions to proceed so Police Scotland / SPA Forensics have a sense of the overall question that needs to be answered in order to move to the next stage of the lifecycle.

This lifecycle approach is intended to be of practical use to project teams in Police Scotland / SPA Forensics and to give senior decision-makers a sense of where a particular project is along this journey. It also provides a natural opportunity for input, review and oversight when moving from one stage to the next.

Developing a data-driven project is often not a linear process and may require moving back or between two stages before moving forward. The lifecycle should be used flexibly, recognising that data-driven tools will require different approaches and will be developed in different contexts.

Diagram 1 below sets out how governance of data use and data-driven technology will work in line with the Project Lifecycle:

- The Ethics Advisory Panels discuss whether Police Scotland *should* use data in a particular way or develop a new data-driven technology at the Problem Identification stage. They should also be identifying the ethical challenges and sorts of mitigations needed if the Service was to go ahead with the project.
- The Data-driven Technology Oversight Group provides internal input and oversight of AI and algorithmic data-driven projects through the project lifecycle.
- Projects that fit the criteria set out in the Introduction will be reviewed and scrutinised externally by the Independent Data Ethics Group from the Design stage through to deployment.
- The Digital and Data Design Authority will provide input specifically at the Design stage.

Ethical questions or challenges associated with a project may be raised by Police Scotland itself or by these bodies as a project progresses. Should a new and sensitive ethical challenge emerge midway through the project lifecycle, it may be necessary to refer it back to a National Ethics Advisory Panel or Independent Ethics Advisory Panel.

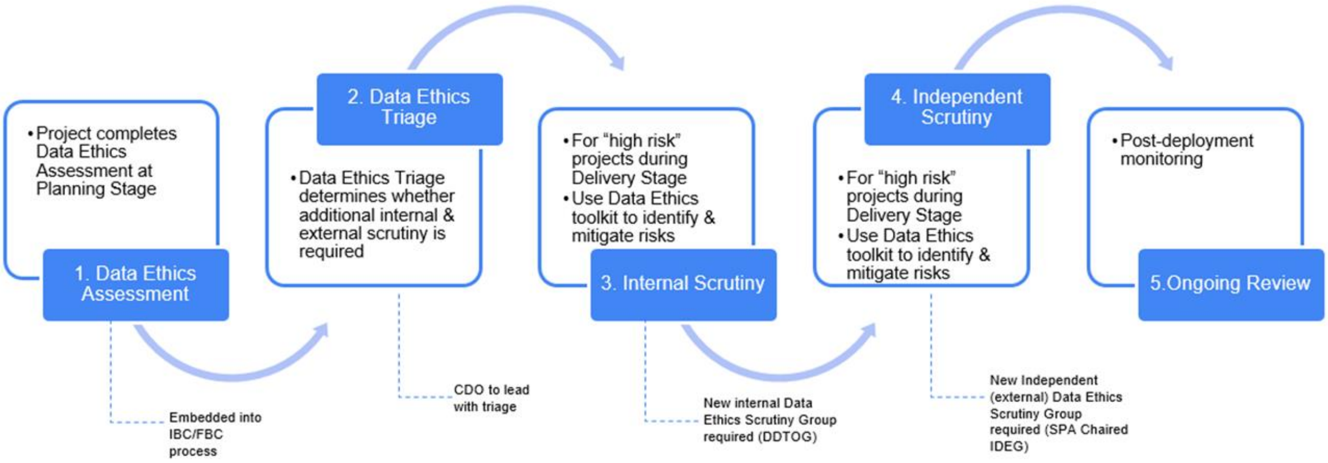
[9] UK Government, 'Agile Delivery', <https://www.gov.uk/service-manual/agile-delivery>, accessed 28 January 2020.

[10] There are different models Police Scotland may like to consider, for example the CRISP-DM approach for data mining.

Part Two of the Framework offers examples of the types of ethical questions which should be considered at each stage of the project lifecycle.

DRAFT

Diagram: Ethics Process



1. Data Ethics Assessment

- Project completes Data Ethics Assessment at Planning Stage

Embedded into IBC/FBC process

2. Data Ethics Triage

- Data Ethics Triage determines whether additional internal & external scrutiny is required

CDO to lead with triage

3. Internal Scrutiny

- For "high risk" projects during Delivery Stage
- Use Data Ethics toolkit to identify & mitigate risks

New internal Data Ethics Scrutiny Group required (DDTOG)

4. Independent Scrutiny

- For "high risk" projects during Delivery Stage
- Use Data Ethics toolkit to identify & mitigate risks

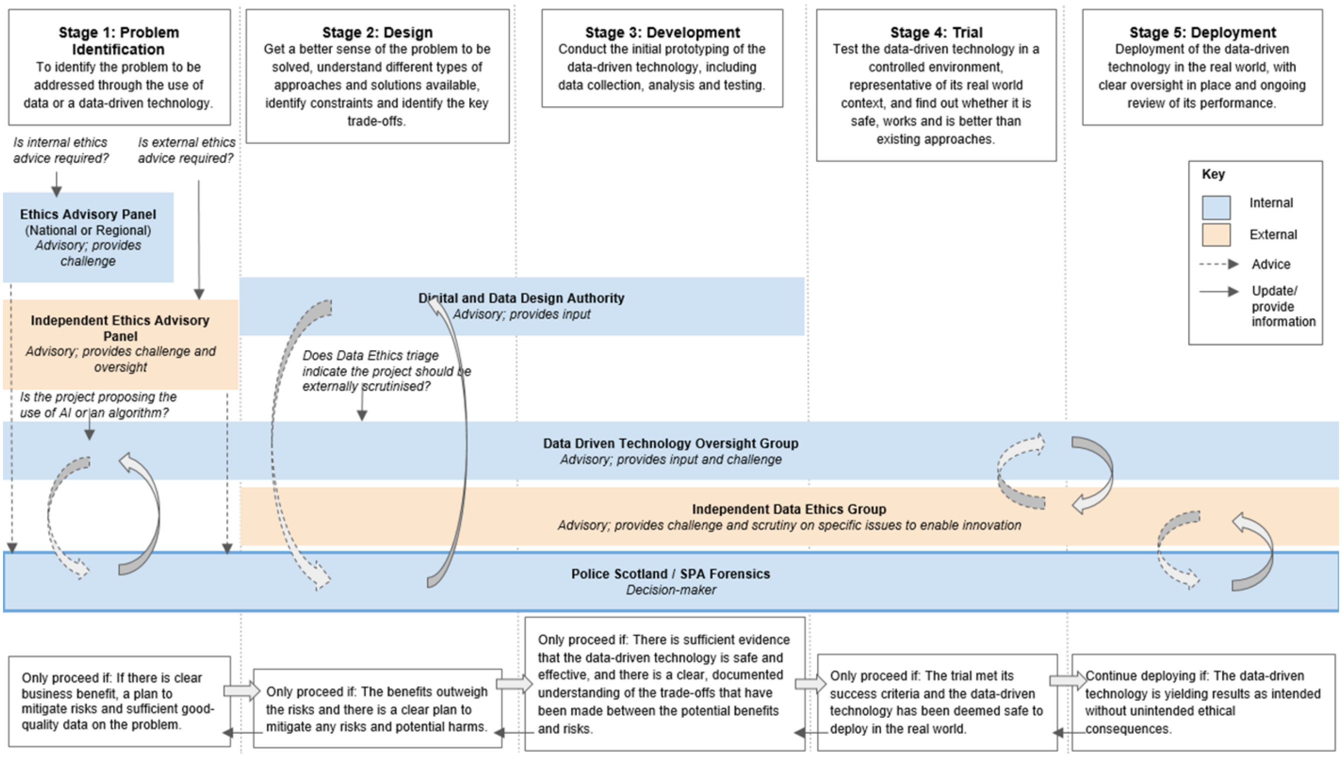
New Independent (external) Data Ethics Scrutiny Group required (SPA Chaired IDEG)

5.Ongoing Review

- Post-deployment monitoring

DRAFT

Diagram: Project Lifecycle



Stage 1: Problem Identification
To identify the problem to be addressed through the use of data or a data-driven technology.

Stage 2: Design
Get a better sense of the problem to be solved, understand different types of approaches and solutions available, identify constraints and identify the key trade-offs.

Stage 3: Development
Conduct the initial prototyping of the data-driven technology, including data collection, analysis and testing.

Stage 4: Trial
Test the data-driven technology in a controlled environment, representative of its real world context, and find out whether it is safe, works and is better than existing approaches.

Stage 5: Deployment
Deployment of the data-driven technology in the real world, with clear oversight in place and ongoing review of its performance.

Is internal ethics advice required?

Is external ethics advice required?

Ethics Advisory Panel
(National or Regional)
Advisory; provides challenge

Independent Ethics Advisory Panel
Advisory; provides challenge and oversight

Is the project proposing the use of AI or an algorithm?

Digital and Data Design Authority
Advisory; provides input

Does Data Ethics triage indicate the project should be externally scrutinised?

Data Driven Technology Oversight Group
Advisory; provides input and challenge

Independent Data Ethics Group
Advisory; provides challenge and scrutiny on specific issues to enable innovation

Police Scotland / SPA Forensics
Decision-maker

Key

🟦	Internal
🟧	External
- - -▶	Advice
——▶	Update/ provide information

Only proceed if: If there is clear business benefit, a plan to mitigate risks and sufficient good-quality data on the problem.

Only proceed if: The benefits outweigh the risks and there is a clear plan to mitigate any risks and potential harms.

Only proceed if: There is sufficient evidence that the data-driven technology is safe and effective, and there is a clear, documented understanding of the trade-offs that have been made between the potential benefits and risks.

Only proceed if: The trial met its success criteria and the data-driven technology has been deemed safe to deploy in the real world.

Continue deploying if: The data-driven technology is yielding results as intended without unintended ethical consequences.

Part Two: Practical guidance for addressing ethical considerations

Overview

Part Two begins with a risk triage for identifying projects with a particularly high degree of ethical risk or complexity. It then leads into a step-by-step lifecycle for such projects, setting out the questions Police Scotland / SPA Forensics should ask at each stage of the project lifecycle in order to identify and address the key ethical considerations that may arise. It also sets out who the key decision-makers are at each stage, who advice can be sought from and what the key check-points and decisions to proceed should involve. The guidance also features examples of the type of advice that should be sought from internal and external experts.

This process should provide a consistent approach for Police Scotland / SPA Forensics to work through methodically. However, it should also remain flexible and be refined as it gets tested on real-life use cases. The project lifecycle approach should also allow for experimentation and testing, in a responsible way, prior to deployment. This step-by-step guidance should also help Police Scotland / SPA Forensics .to engage on specific questions about how a specific data-driven technology is designed, developed or tested along the way. The governance in practice diagram should be a helpful resource to follow alongside the guidance.

Key themes

The Guidance questions are structured by key themes related to the responsible development and use of data and data-driven technology which should be returned to at each stage. The key themes[11] include:

- **Value and impact:** The use of data and data-driven technology should provide value and benefit to individuals or society that is measured and evidenced.
- **Effectiveness and accuracy:** Data-driven technology in policing should be reliable and improve the accuracy of existing approaches. This should be monitored, audited and for particularly sensitive projects independently evaluated. Good quality data is required to ensure the data-driven technology is reliable and effective.
- **Necessity and proportionality:** Any potential intrusion arising from police use of data must be necessary to achieve legitimate policing aims and proportionate in relation to the anticipated benefits.
- **Transparency and explainability:** The project's purpose, details of the data it uses, and notice of its deployment should be made public and open to scrutiny. Data-driven technology should be understood at an appropriate level by relevant individuals using and affected by it.
- **Reliability and security:** Data-driven technology in policing should be reliable and measures should be in place to ensure data is used securely and protects individual privacy.

[11] This builds on CDEI's Trust Matrix developed for its report on public sector data sharing, with some additional considerations for data-driven technologies in the policing context - https://cdei.blog.gov.uk/2020/07/19/addressing-trust-in-public-sector-data-use/

Along with these key themes, **governance and accountability** need to be considered carefully throughout the project lifecycle. The key governance bodies involved in the decision-making have been set out in Part One. Police Scotland and SPA Forensics will need to be clear who is making decisions about the inevitable trade-offs that will arise in addressing the themes above i.e. acceptable levels of efficacy and safety; the benefits versus risks, risks of privacy invasion or bias; and levels of transparency and user control. These decisions and their rationale will need to be documented and mechanisms will need to be put in place to ensure broader societal consent, where individual subjects do not give explicit consent.

Risk Triage

The below sets out eleven questions to be used as part of a triage process, determining which projects should be fed through the step-by-step lifecycle which forms the bulk of the Data Ethics Governance Framework.

Each question can be scored as HIGH, MEDIUM or LOW.

The questions in the approach are intended to be as clear-cut and unambiguous as possible, making it smooth and straightforward to score a particular project. However, the questions are also intended to facilitate a conversation. There is no scientific formula for determining precisely which combination of HIGH, MEDIUM and LOW responses will determine whether a project should be passed from the triage process directly to the Governance Framework, and some projects which ignite fewer HIGH responses than others may nevertheless be determined to be particularly high-risk because of the nature of those answers.

CLUSTER: SCALE QUESTIONS (BREADTH AND DEPTH)

1. **How large in scale is the project (i.e. how many people will the full rollout impact, and what is the depth of that impact)? Will the full rollout directly affect members of the public, and how?**

HIGH: The project will affect members of the public across Scotland, and will affect them directly (e.g. it will affect how they personally interact with or experience the police).

MEDIUM: The project will affect members of the public within a specific city, county or other limited area. Alternatively, the project will affect members of the public across Scotland, but will affect them indirectly (e.g. it will affect how their data is stored or processed).

LOW: The project is not intended to affect members of the public, i.e. it is an internal-only project and will only affect Police Scotland / SPA personnel. (Note that some internal-only projects may still have a significant public interest element, because they signify a major step-change in Police Scotland's capabilities, or how Police Scotland interacts with the public. Question 2 is designed to pick up these projects. Other internal projects may still be controversial, because they have an intrusive, coercive or punitive dimension, such as workplace surveillance projects. The cluster of questions on risks and implications is designed to pick up these projects).

2. **Does the project signify a major step-change in Police Scotland / SPA Forensics' capabilities, or how Police Scotland / SPA Forensics interacts with the public?**

HIGH: The project signifies a major step-change (e.g. it might reshape the core principle of policing by consent; it dramatically alters where human decision-making sits in Police Scotland / SPA Forensics operations; it requires the collection of sensitive data which Police Scotland / SPA Forensics has not previously captured; it involves a significant financial investment).

MEDIUM: The project signifies a medium step-change (e.g. it requires the aggregation or analysis of sensitive data which Police Scotland / SPA Forensics has previously collected but not subjected to this type of analysis; it involves a medium financial investment).

LOW: The project does not signify a major step-change.

3. **Where does human decision-making sit within the outcomes of the project?**

HIGH: The project/ tool will make predictions or recommendations which are automatically implemented.

MEDIUM: The project/ tool will make predictions or recommendations which are used to inform human decision-making.

LOW: The project/ tool will collect or visualise data, but humans will then harness and interpret that data.

4. **How novel is the project?**

HIGH: The project is totally novel – to the best of our knowledge no other police service has implemented a similar project, and Police Scotland / SPA Forensics have not worked on a similar project before. Alternatively, another police service or services have implemented or are piloting similar projects, but have experienced substantial operational problems or controversies.

MEDIUM: Another police service or services have implemented or are piloting similar projects, without substantial operational problems or controversies. Alternatively, such problems or controversies have been mitigated, and Police Scotland / SPA are confident in their ability to learn from and avoid these.

LOW: Similar projects have been implemented by multiple other police services, with no significant operational problems or controversies.

CLUSTER: DATA

5. **What kind(s) of data are to be used in the project, and for what purpose? Note that highly risky or controversial projects may still be more ethical than the alternative because their benefits outweigh the risks; the purpose and benefits statement, and the step-by-step lifecycle, are intended to carefully analyse these questions of necessity and proportionality.**

HIGH: Highly sensitive personal data or highly controversial data or with potential for significant collateral intrusion. Also includes purposes which are particularly challenging or complex to achieve, or likely to ignite significant controversy. For example, sensitive personal data such as health data, data gathered through stop and search, or using historic data to make predictions about individuals' future behaviour.

MEDIUM: Medium-sensitive data and/ or purposes which may be considered controversial or which might raise public concerns. For example, anonymised, aggregated data on crime patterns in a particular area.

LOW: Data and purposes which are not associated with particular controversies or public concerns, and which are not personally identifiable.

6. **How would you categorise the quality and availability of the data required for the project?**

HIGH: Poor. The project involves data which is likely to be poor-quality, incomplete, badly labelled or categorised. And/ or accessing the data in question is likely to be highly challenging.

MEDIUM: Acceptable. The project involves data which is likely to be of average quality or straightforward to get to an acceptable level of quality. And/ or accessing the data in question is likely to be relatively straightforward, or challenges should be easily mitigated.

LOW: Good. The project involves data which is likely to be complete and high-quality, with little or no issues such as duplication or lack of labelling. Police Scotland / SPA Forensics already has access to the data.

7. **Does the project involve data-sharing with other organisations? Is there clear governance in place for data to be shared with third parties/ What does the governance of data-sharing look like?**

HIGH: Yes, the project will involve sharing with one or more organisations in order to combine Police Scotland / SPA Forensics personal data relating to members of the public with that belonging to another organisation to create a new data set that Police Scotland / SPA Forensics may or may not have access to.

MEDIUM: Yes, the project will involve sharing with multiple organisations, including those outside the criminal justice arena where Police Scotland / SPA Forensics have not traditionally had an information sharing agreement. Or, the sharing will be with one organisation but the data will be shared for a different purpose than that for which it was originally collected.

LOW: No, the project does not involve sharing with any other organisation or it involves sharing with criminal justice partners in accordance with well-established sharing processes or on an existing shared platform.

CLUSTER: OUTCOMES/ EFFECTS QUESTIONS

8. **How intrusive, punitive or coercive are the interventions which could result from the project? Consider two dimensions - both the output or resulting action of the tool/ project itself, and policing interventions which could follow from its use e.g. follow-up police actions.**

HIGH: Very (e.g. in-person police interviews or interventions; levels of surveillance which are dramatically different from the existing situation, either in terms of the number of people targeted, or the depth of intrusion; significant alterations in public behaviour).

MEDIUM: Slightly (e.g. similar levels of surveillance to the current situation in terms of the number of people targeted or the depth of intrusion, but with new levels of automation, or new in-person elements; minor alterations in public behaviour).

LOW: Barely/ none. The interventions will not substantially differ from existing approaches.

9. **To what degree could the project encroach on individuals' civil liberties, privacy or human rights?**

HIGH: Significant punitive encroachment, and/ or the encroachment may take place with minimal human intervention (e.g. automated targeted intrusions).

MEDIUM: Medium punitive encroachment, and the encroachment will always be controlled by a human decision-maker.

LOW: No encroachment, or the project is intended to support/ uphold individuals' civil liberties, privacy or human rights, and judgements around this will always be held by a human decision-maker.

CLUSTER: DISPROPORTIONALITY QUESTIONS

10. Does the project involve objectives that academics, civil society, the Government, media or members of the public have voiced concerns about in the past, which in turn suggest that there might be problems with public acceptability of the project?

HIGH: Yes, recent concerns have been raised from multiple sources (e.g. similar projects run by other police services have generated media criticism, academics have published research highlighting potential problems, social media discussion is heated, there is significant attention but the technology itself is not well-understood).

MEDIUM: Yes, recent concerns have been raised by one (reputable/ high-profile) source.

LOW: No concerns have been raised which Police Scotland / SPA Forensics is aware of (assuming a reasonable level of effort to identify such concerns).

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?

HIGH: Yes. The project may be specifically designed to target particular groups. Alternatively, multiple sources (academic research, reports, Police Scotland / SPA Forensics analysis) may suggest that certain groups will be affected more than others.

MEDIUM: Potentially. The project may not be specifically designed to target particular groups, but there is a risk that it will affect some more than others. One or more sources may suggest that certain groups will be affected more than others.

LOW: No, there is no evidence to suggest that certain groups will be affected more than others (assuming a reasonable level of effort to identify such concerns), and the project has not been designed to target specific groups.

Stage 1: Problem Identification

Summary

- ➢ **Objective:** To identify the problem to be addressed through the use of data or a data-driven technology
- ➢ **Decision-maker:** Police Scotland / SPA Forensics Senior Responsible Owner
- ➢ **Question to proceed to the next stage:** Is there clear business benefit, a plan to mitigate risks and sufficient good-quality data on the problem? Is the use of a data-driven approach necessary and proportionate to achieve legitimate policing aims?
- ➢ **Advice can be sought from:** Police Scotland Ethics Advisory Panels, Data-driven Technology Oversight Group
- ➢ **Supporting documents to be completed**: Business case

Overview

Police Scotland and SPA Forensics regularly encounters a range of problems which could be addressed through the use of data or a data-driven technology. At this stage, they need to identify the problem to be addressed through such use. Examples of these problems could be: How can we best estimate staff resourcing requirements and suggest appropriate shift patterns? Or how can we work out what affects incident volumes and produce a forecast that accounts for these effects? A range of individuals should also be consulted on the problem, to ensure the right problem is prioritised and there is no bias in the problem selection.

Key questions

In order to work out whether the problem is suited to a data-driven technology and what the key ethical considerations are, Police Scotland / SPA Forensics should answer the following questions:

Value and impact

- What is the business benefit and value of the data-driven project, and how will that value be defined? Is there clear evidence to suggest that a data-driven approach is likely to offer tangible improvements when compared to a non-technological alternative? (e.g. cost savings, improvements in accuracy of decision-making etc.)
- What are the possible risks?
- What might the intervention(s) resulting from the data-driven technology be?
- What type of data-driven tool or model could be used to address this problem? For example, is it an explanatory or predictive model? Does the tool already exist or would it need to be developed internally or procured?
- Is ring-fenced resource for experimentation, innovation or process improvement available, which could be applied to this project?
- What is the policing purpose justifying the use of data analytics: both its means and ends? (ALGO-CARE)

The data

- What type(s) of data would be needed to tackle this problem?
- Do Police Scotland / SPA Forensics already have access to such data? If not, or if the existing data is insufficient, does the police force need to collect further data itself, or are there other bodies holding such data which could share it? In such cases, what are the

implications of accessing those datasets/ sharing data with the third party in question?
- What sort of quality issues might there be with this data i.e. gaps, over-representation of certain groups, labelling inconsistencies?
- Are Police Scotland / SPA Forensics maximising the value of the data they already hold, or are there opportunities to go further i.e. might it be unethical to *not* implement data analytics?
- Could there be data maximisation or other benefits from conducting this work in a separate environment as far as possible from normal police operations?

Transparency and explainability

- How have individuals or groups from across Police Scotland / SPA Forensics assisted in identifying and refining the problem? This might include engagement with specialist ethics panels or committees, depending on the structure of the force in question.
- How will the public or affected groups be engaged throughout the project? As above, this might include engagement with specialist external panels, or ongoing public engagement initiatives.
- Will the problem and its solution require an external communications programme, for example because it is particularly sensitive or public-facing? What should this look like?

Effectiveness and accuracy

- What expertise will be needed to design and develop this technology?
- How will effectiveness and accuracy of the data-driven project be understood/ measured?
- How will the tool be tested and evaluated before it is deployed?

Necessity and proportionality

- Is the use of a data-driven approach necessary and proportionate to achieve legitimate policing aims?
- What is the purpose for collecting or repurposing the data, and would using the data for this analysis be lawful, necessary and proportionate?

Reliability and security

- What are the potential consequences if the system malfunctions or fails to operate reliably?
- What safeguards will be needed to prevent improper use of the system?
- How will the data be stored and what are the processes required to ensure security of the data and the system?

Advice

Depending on the type of problem or proposed data-driven technology, Police Scotland may want to seek internal or external ethics advice from its National, Regional or Independent Ethics Advisory Panels. As Police Scotland starts to consider predictive analytics tools, for example, it may want to ask the Independent Ethics Advisory Panel what its members think the key ethical considerations that would need to be addressed are.

At this stage, it will often not be possible to determine with precision the benefits or risks as this will depend on the outcomes of the development work. However, there should be sufficient evidence either from operational experience or from the implementation of systems by others that warrant further investment in pursuing this possibility.

If the type of data-driven technology being discussed may employ algorithms or AI, Police Scotland / SPA Forensics may wish to seek input and challenge from the Data-driven Technology Oversight Group.

DRAFT

Question to proceed

Ultimately, the decision to move to the next Stage (Design) should be made by the relevant SRO. They will need to complete a business case, which answers the questions above along with completing any existing assessments which look at how the project would fit with business and operational priorities.

Stage 2: Design

Summary

- ➢ **Objective:** Get a better sense of how to solve the problem, understand different types of approaches, determine what data should be used, and identify constraints.
- ➢ **Decision-maker:** Police Scotland / SPA Forensics SRO
- ➢ **Question to proceed to the next stage:** Do the benefits outweigh the risks regarding moving to the next stage and is there a clear plan to mitigate any risks and potential harms?
- ➢ **Advice can be sought from:** Digital and Data Design Authority, Data-driven Technology Oversight Group, Independent Data Ethics Group
- ➢ **Documents to be completed**: Project Design report; Data Protection Impact Assessment, Equality & Human Rights Impact Assessment, Community Impact Assessment (see Annex 3).

Overview

At the Design stage, Police Scotland / SPA Forensics needs to get a better sense of the problem it is trying to solve, understand different types of approaches and solutions available, determine what data should and should not be used to build the tool, identify constraints and identify the key trade-offs. This is about designing the approach to developing a tool, rather than the design of the actual system which is part of the development and testing phase. If Police Scotland / SPA Forensics is considering commissioning a private sector provider or partner to develop the data-driven solution, it is critical that there is sufficient understanding of the underlying methodology and its limitations to ensure that it is integrated into operational processes in an appropriate way.

Key questions

In order to identify the key ethical considerations at this stage, Police Scotland / SPA Forensics should answer the following questions:

Value and impact

- Is it intended that the data analytics be used to make decisions or will they inform decisions made by police officers and staff?
- What are the proposed benefits, purpose and resulting intervention of the project?
- If the project will lead to new interventions or affect existing police operations, what would be the required resource to deliver these?
- What are the risks that could come about through the project, including risks identified in the Data Protection Impact Assessment (DPIA), and what is the plan to monitor and mitigate these?
- What risks have the Equality & Human Rights, and Community Impact Assessments identified and how will these be monitored and addressed?
- What, if any, are the trade-offs between benefits and risks, and how will those trade-offs be communicated to relevant parties?

The data:

- What data subjects will the project involve? Roughly how many are there and how will they be categorised?

- Will the tool process personal data or special category personal data? Will data be anonymised or pseudonymised prior to analysis?
- Have data standards been established to ensure any data collected is reusable and interoperable?
- Have existing/ acquired datasets been assessed for quality in terms of incomplete data, duplicate data, inconsistent formatting, and issues with data quality or bias? How are such problems to be mitigated?
- Has due consideration been paid to ensuring that the tool collects the minimum amount of data?
- Will the proposed activity require any consultation with data subjects? Does the proposed activity involve engaging with service users or members of the public?
- Have effective safeguards been put in place to protect individuals' privacy and confidentiality?
- What is the proposed retention schedule for the data?
- Is data processed by the algorithm lawfully obtained, processed and retained, according to a genuine necessity with a rational connection to a policing aim? (ALGO-CARE)
- Is data categorised to avoid 'broad-brush' grouping and results, and therefore issues of potential bias? Is the provenance and quality of the data sufficiently sound? (ALGO-CARE)

Effectiveness and accuracy

- What expertise is required to build the data-driven technology and ensure appropriate legal and ethical review? What different approaches to model development should be tested in the development stage? How will their relative merits be assessed?
- What are the evaluation criteria for the project, and what minimum standards will the product need to meet for operational deployment?
- What level of red-teaming or external challenge should be put in place to robustly test different approaches during the development phase?
- How will the effectiveness of the data-driven technology be assessed during the testing phase?
- How will the effectiveness of the technology be measured? How will independent auditing, monitoring and evaluation of the technology work?
- How will failure rates be measured, and what failure rates are acceptable?
- What additional training may be required for the users of the tool, to ensure they can use it responsibly in conjunction with their own professional judgement?

Necessity and proportionality

- Why is this use of data analytics suitable, necessary and proportionate for addressing the problem?
- Is the potential interference with the privacy of individuals necessary and proportionate for legitimate policing purposes? (ALGO-CARE)

Transparency and explainability

- Does a Privacy Notice exist for this processing, explaining to data subjects how their data will be processed?
- If not exempt from FOISA requests, has information regarding the proposed project been made publicly available on the force website? If not, why not?
- Would disclosing the existence of this technology potentially compromise operational capabilities? If so, has legal counsel advised that information relating to this project would be exempt from FOISA requests?
- Will the project involve complex statistical modelling (e.g. machine learning)? If so, what level of explainability will the algorithm be able to provide, particularly regarding the relative impact of input variables on the resulting output?

- If procuring a commercial/ off the shelf system, what transparency and explainability requirements need to be stipulated in the contract with the provider?
- What additional information will users of the system need in order to operate it responsibly?
- Do you know if other UK police forces / forensic services providers have tried to address a similar problem and, if so, have you spoken to them to share lessons?
- Have you considered any additional groups who you do not regularly engage with who might be affected by the technology? To what extent do you have existing relationships or a way to reach these groups?
- Is the tool likely to form part of a decision-making process that may need to be evidenced in court? If so, are there minimum evidential standards that must be met in the design of the system, e.g. those set by the Forensic Science Regulator?

Reliability and security

- What measures are in place to ensure data is used securely and appropriately protects individual privacy?
- What are the potential consequences if the system malfunctions or fails to operate reliably?
- What safeguards will be needed to prevent improper use of the system?
- What access controls are required to restrict who has access to the system?
- What would be the consequences if this tool fell into the wrong hands? Are additional restrictions required to prevent this from happening (e.g. security classification, compartmentalised systems etc.?)
- What are the key privacy concerns? If it is decided that the tool must prioritise preserving privacy, is there an understanding of how this could undermine the tool's effectiveness?
- What purpose was the data originally collected for? Will consent be required to capture the data?
- Will the tool use identifiable data or will it be anonymised?

Advice

At this stage, Police Scotland can seek internal input and advice from the Technical Design Authority. It can also seek input and challenge from the Data-driven Technology Oversight Group which may have already discussed the project at the Problem Identification stage. Where external challenge and scrutiny is needed, given the sensitivity, complexity or novelty of the tool being proposed, the project should be taken to the Independent Data Ethics Group. Police Scotland should also seek advice from other police forces in the UK who have done similar projects and externally, from academics and researchers.

Decision to proceed

The decision to proceed should be made by the Project SRO, taking into account the advice sought. The decision to proceed to the next stage should be based on whether a) the likely benefits outweigh the potential risks at this stage (not yet for operational deployment); b) there is a clear plan to mitigate any risks and potential harms; c) the lawful basis for proceeding with the project has been established and clearly documented. The likely risks at this stage could be:

- The data is not good enough/ sufficiently good quality data cannot be accessed.
- There is not sufficient expertise (or clear access to it externally) for product development.
- The data cannot be managed in a secure environment that would allow the right work to be done to it.
- Use of such a tool would not be a lawful or legitimate use of police powers.
- An impact assessment has identified unacceptable risks that cannot be managed appropriately within the parameters of the project.
- The expected benefits of the tool are not significant enough to justify the resource investment required to continue with the project.

This is the stage at which a robust testing of public attitudes (through research or engagement) could be undertaken to prevent any further spending on something where public acceptability was found to be too low to warrant further work.

If Police Scotland / SPA Forensics do not feel it has a clear plan to mitigate these risks, the relevant SRO can return to the Problem Identification stage to redefine the problem, or bring the project to a close.

Stage 3: Development

Summary

- ➢ **Objective:** Conduct the initial prototyping of the data-driven technology, including data collection and analysis. Think about how the technology will be used by police staff and the levels of transparency and explainability required given the context
- ➢ **Decision-maker:** Senior Lead at Police Scotland / SPA Forensics
- ➢ **Question to proceed to the next stage:** Is there sufficient evidence that the data-driven technology is safe and effective, and is there a clear, documented understanding of the trade-offs that have been made between the potential benefits and risks?
- ➢ **Advice can be sought from:** Digital and Design Authority,, Data-driven Technology Oversight Group, Independent Data Ethics Group
- ➢ **Documents to be completed**: Report on accuracy and effectiveness of the data-driven technology; Updated Impact Assessments

Overview

At the Development stage, the data will be collected, analysed and tested, and the data-driven technology will be tested for its accuracy and effectiveness and how it would be presented visually to users. Greater independent oversight and scrutiny is likely to be required from the Independent Data Ethics Group to interrogate the accuracy and effectiveness of the technology. Moreover, external expertise from data scientists, analysts, lawyers and ethicists may need to be sought.

Difficult decisions will have to be made about what acceptable levels of efficacy and safety are and where Police Scotland / SPA Forensics will come down on the trade-offs between benefits and risks, including risks of privacy invasion or bias; levels of transparency and user control. These discussions and decisions will need to be documented and, where possible, put into the public domain.

Key questions

In order to identify the key ethical considerations at this stage, Police Scotland / SPA Forensics should answer the following questions:

Value and impact:

- Is the proposed/ prototyped solution still necessary and proportionate to achieve the goals of the project?
- What understanding is there about the population(s) which will be affected (or whose data is being used) by the data-driven technology? How could Police Scotland / SPA Forensics best engage with them before deployment?
- Could using this data protect other people i.e. what is the likely community benefit?
- If developing an algorithm, what statement has been developed to define fairness in the context of its use?[12]
- Do the expected benefits of using the technology outweigh the resources required to develop and maintain it?

Effectiveness and accuracy:

[12] You may wish to draw on the guidance produced by the Alan Turing Institute - Understanding artificial intelligence ethics and safety - recommends drawing up a Fairness Position Statement. The position statement then drives the detection and mitigation of bias.

- What is an acceptable accuracy rate for the technology? What will be the effects of it making "wrong" recommendations?
- What is the ratio of false positive to false negative errors? What would a false positive or false negative mean in the context of the technology?
- Have you tested your approach to model development with external experts? Are you testing multiple potential approaches? Have you created red teams to challenge the proposed approach and attempt to identify weaknesses or improvements?
- Has the development process identified any potential biases in the data or the modelling? If so, what additional measures can be introduced to minimise risk of bias?
- Has there been an assessment of internal capacity and capability needed to develop and deploy the technology?
- If developing an algorithm, could any variables in the tool serve as proxy measures for the protected characteristics? If so, has the data been analysed to demonstrate the extent of any correlation between the potential proxy and the protected characteristic?
- If using a machine learning algorithm, what processes are in place to ensure retraining and re-validation of the model over time?
- In what way will the tool improve the current system and is this demonstrable? (ALGO-CARE)

Transparency and explainability:

- To what extent is the evidence of efficacy and privacy open to independent scrutiny through open source code and scientific evaluation (for internally developed tools) or information on third-party suppliers (for Commercial Off-The-Shelf (COTS) tools)? Are there routes for this, in particular for those affected by the decisions?
- What would a pre-test notice look like? What would the plan be to publish this or notify those who may be directly affected?
- What engagement has there been with frontline police officers and users? How will the tool be tested with them to ensure it is intuitive and supports them?
- If an algorithm, does it make suggestions at a sufficient level of detail/granularity, given the purpose of the algorithm and the nature of the data processed? (ALGO-CARE)
- Is appropriate and intelligible information available about the decision-making rule(s) and the impact that each factor has on the final score or outcome? (ALGO-CARE)

Reliability and security:

- Has there been an opportunity for all parties involved to voice their concerns around the potential data sharing risks?

Advice

At this stage internal advice and challenge can be sought from the Data-driven Technology Oversight Group and external challenge and oversight from the Independent Data Ethics Group.

Advice: False positives and false negatives with algorithms

No predictive tool can achieve 100% accuracy, meaning that there will always be instances of underestimation and overestimation of risk. For example, in the case of an algorithm designed to predict risk of reoffending, some individuals will be predicted as likely to reoffend, who would not have gone on to do so, and vice versa. These two types of error are referred to as Type 1 and Type 2, or false positives and false negatives.

The design of an algorithm will attempt to minimise both types of error, but there will ultimately be trade-offs between reducing under and over prediction of risk. Both kinds of error have the potential to cause harm. If a tool consistently underestimates risk of reoffending, there may be cases where dangerous individuals are inappropriately released from custody. On the other hand, if risk is overestimated, individuals may be excessively penalised causing harm to them.

The decision of where to set risk thresholds and the consequent ratio of false positives to false negatives is a human one and a particularly important decision in policing given the human and public safety consequences. The decision can be framed as balancing potential societal harms (e.g. of releasing an individual who goes on to reoffend) against potential individual harms (falsely categorising an individual as likely to reoffend). When designing and deploying these tools, individual forces will need to consider how they establish an appropriate balance between these kinds of potential harm.

Advice: Protected characteristics, proxies and whether to include as input variables

The protected characteristics set out in the Equality Act 2010 are an important starting point for ensuring tools do not unduly discriminate against certain classes of individuals. It is common practice to avoid using data on protected characteristics as inputs into a tool, as to do so may be illegal. However, in the context of policing and depending on the type of tool being developed it may be important to include certain protected characteristics such as sex and age in order to reflect the way that crime is patterned across different demographics.

Removing protected characteristic data from a tool does not remove the possibility that other data might serve as an effective proxy for a characteristic (and sensitive data under the Data Protection Act). For example in policing, home address or number of stop-and-searches could serve as proxies for ethnicity (the use of Stop and Search data is discussed in Box 12).

Another consideration is that the protected characteristics listed in the Equality Act may not cover all sensitive data points identified by an algorithm, for example socio-economic background. This is particularly relevant to the policing context where individuals from disadvantaged socio-demographic backgrounds are likely to engage with public services more frequently, meaning the police often have access to more data relating to these individuals, which may in turn lead to them being calculated as posing a greater risk.

Decision to proceed

Given the next stage would involve the testing (in a deployment context) of the data-driven technology, Police Scotland / SPA Forensics should:

- Assign a senior point of accountability to sign-off the test.
- Be satisfied that the model has been tested against criteria for bias, accuracy and reliability and has passed the necessary thresholds to proceed.
- Be satisfied with the evidence provided that the data-driven technology is safe and effective.
- Understand the mitigations in place to address risks and potential harms and the impact these will have on the potential benefits and effectiveness of the data-driven technology.

Depending on the results of those tests, the project may need to return to this Development stage for further refining and adjustments.

Stage 4: Testing

Summary

- **Objective:** Test the data-driven technology in a controlled environment, representative of its real world context, and find out whether it is safe, works and is better than existing approaches.
- **Decision-maker:** Senior Lead at Police Scotland/ SPA Forensics
- **Question to proceed to the next stage:** Has the test met its success criteria and has the data-driven technology been deemed safe to deploy in the real world?
- **Advice can be sought from:** Data-driven Technology Oversight Group, Independent Data Ethics Group
- **Documents to be completed**: Test report, Updated Impact Assessments

Overview

Controlled testing is essential before moving ahead with large-scale deployment. By ensuring there is clear evidence that a data-driven technology is effective and delivering results in the testing phase, Police Scotland / SPA Forensics will be better able to evaluate the tool before rolling it out in the real world. The approach to doing this will depend on the technology being developed and may include:

- Running new systems in parallel to existing ones on a common population (if possible) to assess differences in outputs and provide a failsafe mechanism
- Testing a data-driven intervention in a limited geographic area
- Passing data-driven insights to police officers and Police Scotland / SPA Forensics staff over a limited time period, and assessing the extent to which use of the data-driven insights is improving the quality of police decision-making.

It is also critical for a test to have the possibility of yielding a negative result. There should be clear success criteria for the test and, if it fails to meet these, the intervention should not be rolled out more widely without further development and retrial.

In the case of predictive tools, there are ethical issues to be considered with randomised control testing given it would be unethical not to intervene if the tool suggests an individual is highly likely to commit a violent act, for the purpose of determining whether the prediction was accurate.

Key questions

In order to identify the key ethical considerations at this stage, Police Scotland / SPA Forensics should answer the following questions:

Value and impact:

- What lessons can be learnt from tests conducted by other police forces / agencies with similar data-driven technologies?
- At which points will the internal or external oversight bodies be able to review test progress? What are the key decision points throughout the test?
- Are the initial test findings bringing up any ethical issues with the purpose or design of the data-driven tool which need to be discussed? Should the tool be returned to the Development stage for adjustment, refinement or wholescale redevelopment?
- Who owns the tool and the data analysed? Does the force need rights to access, use and amend the source code and data analysed? How will the tool be maintained and updated? Are there any contractual or other restrictions which might limit accountability or evaluation? (ALGO-CARE)

- Post-test: Does the benefits statement need to be amended? Have new risks or challenges emerged? Have the benefit/ risk trade-offs altered?
- Post-test: Is the type of data-driven technology or technique proposed likely to do what is intended and deliver on the value proposition?

Effectiveness and accuracy:

- Pre-test: How have success criteria for the alpha and beta tests been defined?
- Pre-test: How will it be assessed if the intervention causes harms or unintended consequences?
- Pre-test: How will it be proved that the intervention offers substantial improvements over processes, for example by giving greater accuracy or efficiency?
- How does the environment the data-driven technology is being tested in differ to the real-world? What will need to be addressed or monitored to ensure the performance of the data-driven technology adapts well to the deployment context?
- What plan is there to train users on how the data-driven technology works? Is there sufficient funding for this training and has it been factored into the timings prior to deployment?
- How will data be collected for monitoring purposes?
- Are any improvements in effectiveness or efficiency proportionate when balanced with the resources required, and the level of intrusion arising from the use of the tool?
- Has the Police Scotland / SPA Forensics satisfied itself that everything reasonable has been done in order to make sure the tool does not have unacceptable bias on the grounds of protected characteristics?

Transparency and explainability:

- How can the test be best set up to ensure progress can be monitored transparently?
- Has information about the test been circulated internally? Are there clear mechanisms in place for individuals to get in touch with those running the test to ask questions?
- Has a communications package been developed for the launch of the test? Does this include mechanisms for interested parties to ask questions or raise concerns? Does it include consideration to communications if the test fails, or raises new risks or challenges?
- Is any proactive engagement planned to be carried out during the testing stage? (e.g. with affected communities, civil society organisations or the media)?
- Would an individual who has not been involved up until now be able to access information about the test and process so far and understand how the tool has been designed?
- Will the results of the testing and evaluation process be published openly on the force website?

Reliability and security:

- Pre-test: Have any real-world impacts on individuals that might result from the test been considered? Have individuals concerned been made aware of this and given the opportunity not to participate?
- Should real police data be used for the test? What are the alternatives? For example, could synthetic data that is generated for the purposes of the test be used?
- What has the test demonstrated about the quality of data being used? Is new or additional data required?
- How are you ensuring the ongoing integrity and security of the tool and the data it uses (and handling it appropriately)?

Advice

DRAFT

Advice should continue to be sought from the Data-driven Technology Oversight Group and the Independent Data Ethics Group. An independent evaluator may also need to be brought in to assess the test results.

Decision to proceed

In order to move to deployment, Police Scotland / SPA Forensics should be satisfied:

- The tests have met their success criteria (and any issues that have emerged have been addressed);
- The tool or technology is safe to deploy in the real world;
- It has the approval of the Chief Constable, or senior leadership, depending on the nature and scale of the technology being deployed; and
- The prototype has been tested against criteria for bias, accuracy and reliability and has passed the necessary thresholds to proceed.
- The users of the product have been adequately trained on how to operate it responsibly in conjunction with existing organisational processes. .

Stage 5: Deployment

Summary

- ➢ **Objective:** Deployment of the data-driven technology in the real world, with clear oversight in place and ongoing review of its performance.
- ➢ **Decision-maker:** Police Scotland / SPA Forensics SRO
- ➢ **Question to continue deployment:** Is the data-driven technology yielding results as intended without unintended ethical consequences?
- ➢ **Advice can be sought from:** Data-driven Technology Oversight Group, Independent Data Ethics Group
- ➢ **Documents to be completed**: Updated Impact Assessments published; notice of deployment published.

Overview

Prior to deployment, the decision to deploy, along with details of the data-driven technology, should be formally recorded and made public. With the data-driven technology in deployment there will need to continue to be a senior point of accountability to oversee how it operates in the real world. This may continue to be the same SRO from before, or perhaps it will sit with someone else in the organisation more directly responsible for the relevant operational area. This individual must have sufficient decision-making power and seniority to draw attention to any serious issues and, if needed, halt deployment. There should continue to be internal and external oversight of the data-driven technology which reviews how it is working in the real world.

Key questions

In order to identify the key ethical considerations at this stage, Police Scotland / SPA Forensics should answer the following questions:

Value and impact

- Is the technology being used in the way intended? How is this being monitored?
- How often will the impact the tool or technology is having be measured and communicated internally and externally?
- What impact is the technology having on how users act? Has it changed their behaviour or decision-making and are there ways of monitoring and evaluating this?
- On an ongoing basis, are the improvements in effectiveness and efficiency proportionate to the resources required and the level of intrusion arising from the use of the tool?
- In the case of an algorithmic tool, is the assessment made by the algorithm used in an advisory capacity? Does a human officer retain decision-making discretion? What other decision-making by human officers will add objectivity to the decisions (partly) based on the algorithm? (ALGO-CARE)

Effectiveness and accuracy:

- Is the technology performing in the way intended?
- Who is using the technology? Has it changed their decision-making and use of discretion? How is this being monitored?
- How is data being collected for monitoring purposes?
- For particularly controversial or sensitive technologies, what is the plan for independent evaluation of its performance and outcomes? This should address how ongoing monitoring

and evaluation will take place, along with a more formal independent evaluation process.

- What approaches are there in place to validate the technology? For example, statistical tests being run to ensure accuracy and mitigate against bias.
- Can the stated accuracy of the algorithm be validated reasonably periodically? Can the percentage of false positives/negatives be justified? (ALGO-CARE)

Transparency and explainability:

- Is the data analytics tool sufficiently understood by all users so that they know the data it is developed on and how it works?
- Where possible has training material, for example an on-demand training video, been made available through the police intranet?
- Are police officers / staff reporting any challenges with using the data analytics tool? Is there reluctance from any police officers / staff to use it?
- Are there mechanisms in place to allow for reporting of any issues, with options for anonymous reporting if necessary?
- Is information on current usage of the data analytics tool up to date and is it easy for external observers to distinguish between approaches which are being tested and those which are fully deployed?
- Are there open channels with journalists and civil society organisations and are they accurately representing the technology in media articles and reports?
- Are there protected channels in place to allow members of the public to report any concerns they have and are there agreed response times to these?
- What are the post-implementation oversight and audit mechanisms? For example, where an algorithmic tool informs criminal justice disposals, how are individuals notified of its use (as appropriate in the context of the tool's operation and purpose)? (ALGO-CARE)

Reliability and security:

- What checks are being made on the quality of any new data being generated by the data analytics tool? Are there mechanisms in place to ensure this is not providing an incomplete or biased picture of the problem the tool is trying to address?
- How are you ensuring that new insights and data are being incorporated into the data analytics tool?
- What is in place to ensure data is consistently being used securely and protects individual privacy?

Advice

Advice should continue to be sought internally through the Data-driven Technology Oversight Group and externally from the Independent Data Ethics Group. Updates on progress and reports explaining the impact the data-driven technology is having on police services should be shared with the Independent Data Ethics Group.

Advice: Using the Policing Evaluation Toolkit

The College of Policing's What Works Centre has developed a helpful toolkit for thinking through an evaluation. This brings together evaluation design and implementation strategies that can be used by practitioners to design evaluations.

Developing a plan for how to evaluate a project from the outset will enable officers and staff to answer the questions 'Did it work?', 'To what extent did it work?', 'Why and how did it work?' It should also provide a framework for knowing whether an intervention was effective or not and assessing the strength of the impact. Moreover, it should allow police forces around the country to better share and use evidence of what has worked elsewhere and test out new initiatives with a robust evaluative framework in place. It can also help save time, resources and money, as it allows knowledge of effective practice to be built up to inform future action and decision-making for maximum public benefit.

The College of Policing considers evaluation a key component of an Evidence-Based Policing approach in which police officers and staff create, review and use the best available evidence to inform and challenge policies, practices and decisions.

Decision to continue deployment

In order to continue deploying the tool Police Scotland / SPA Forensics should regularly be sure that:

- The data-driven technology is yielding results as intended.
- There are no unintended ethical consequences.
- The use of the tool or technology continues to be necessary and proportionate to achieve legitimate policing aims.

Annexes

Annex 1: NPCC sub-categories of data-driven technology

Sub-category	Definition	Existing Police Scotland use cases	Potential future use cases[13]
Biometrics	Information about an individual's physical, biological, physiological or behavioural characteristics which is capable of being used, on its own or in combination with other information (whether or not biometric data), to establish the identity of an individual[14] i.e. DNA, fingerprints and images	Biometric data is collected on each arrested person	Retention?
Cyber and Digital Forensics	The application of science to the identification, collection, examination and analysis of electronic data whilst preserving the integrity of the information and maintaining the chain of custody of that data[15] i.e. mobile device forensics, forensic data	Cyber-kiosks (desktop computers, to enable police officers to view information stored on a mobile phone or tablet, which may be relevant to a police investigation or incident)	Networking of cyber kiosk Child Abuse Image Database (CAID) - images fall under biometrics
Surveillance and Investigatory Powers	The monitoring, observing or listening to persons, their movements, conversations or other activities and communications i.e. through CCTV, body-worn video, ANPR, unmanned aerial systems.	Remote controlled aircraft systems Body-worn videos	
Artificial Intelligence (AI) and algorithms	AI is an umbrella term for a range of technologies aimed at replicating human intelligence abilities in digital computers. AI currently refers mainly to systems that use machine learning for pattern detection, prediction, human-	Basic algorithms used in back-office functions (HR and Finance) 'Civtech challenge': A natural language processing algorithm which sorts through	An algorithm to predict the effect that weather and seasonality has on the number of incidents. An algorithm to predict staff resourcing requirements and

[13] These are hypothetical examples being considered, but not currently deployed, by Police Scotland at the time of drafting this Framework.

[14] https://www.legislation.gov.uk/asp/2020/8

[15] https://www.app.college.police.uk/app-content/investigations/forensics/#digital-forensics

	machine dialog, and robotic control.[16] A set of precise instructions that describe how to process data, typically in order to perform a calculation or solve a problem.[17] Examples include: predictive analytics, algorithmic-support tools.	multiple unstructured data sources coming from logs and notes	suggest appropriate shift patterns.

Annex 2: Existing external governance bodies

The Independent Ethics Advisory Panel (IEAP) is the external arm of Police Scotland's three-part Ethics Advisory Panel. As with the internal panels, the IEAP is not a decision-making forum, but a supportive mechanism. The IEAP is chaired externally and membership is formed from a broad range of groups and organisations representing the public, private and voluntary sectors as well as academia in Scotland. Whilst the ethical challenges submitted for discussion to the IEAP do not have to relate to the use of data and technology, many of the sessions to date have been on this subject. It is likely these issues will continue to be debated by the IEAP along with ethical questions about the way Police Scotland should use data and the types of technologies it should invest in.
The **Scottish Police Authority (SPA)** holds Police Scotland to account and is a public body of the Scottish Government. With regards to the use of data and technology, the SPA requires information and reports from the Chief Constable in order to assess Police Scotland's progress against objectives. The SPA also provides forensic services to Police Scotland, which are separate from the Chief Constable's direct line of command. Given the SPA's accountability role, any external governance and oversight of Police Scotland's use of data should be closely aligned with or be led by the SPA, hence why this Framework recommends the Independent Data Ethics Group is run by the SPA.

The Scottish Government's Justice Sub-Committee on Policing is a Committee of the Scottish Parliament which considers and reports on the operation of the Police and Fire Reform (Scotland) Act 2012 as it relates to policing. The Justice Sub-Committee has a keen interest in how Police Scotland uses technology. For example, it published a report in February 2020 advising Police Scotland against deploying live facial recognition software. Moreover, the Justice Sub-Committee holds debates on the legal and ethical considerations related to police technology, for example body-worn videos and RPAS.

The Scottish Government has recently set up an **Independent Advisory Group (IAG) on New and Emerging Technologies**. This group has been tasked with scoping the legal and ethical issues arising with new and emerging technologies, including the potential impact of new devices and new data handling or processing techniques. At the time of developing this Framework, the remit and scope of the IAG was being defined and it was yet to be convened. The Scottish Government has also set up a **Data and Intelligence Network** to bring together expertise on ethics, governance, engagement and open government to ensure public sector organisations, ranging from health,

[16] https://www.gov.uk/government/publications/cdei-review-of-online-targeting
[17] https://www.gov.uk/government/publications/cdei-review-of-online-targeting

education, policing and social services, are equipped to make responsible decisions about the use of data.

The **UK ICO's Scottish office** main focus is data protection, for which the ICO is the sole regulatory body in Scotland. The UK ICO is a regulator with enforcement powers, which sets it apart from the bodies above. However, it has also published a toolkit for organisations considering using data analytics[18], specifically for law enforcement processing under Part 3 of the Data Protection Act 2018 which Police Scotland should draw on when developing new data analytics tools. In turn, the Scottish Information Commissioner is the independent public official responsible for promoting and enforcing Scotland's freedom of information (FOI) law.

Annex 3: Overview of Impact Assessments

Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.

It is a mandatory process designed to help manage the risks to the rights and freedoms of individuals resulting from the processing of their personal data, by assessing them and determining the measures to address them. Consequently, a DPIA will describe the processing and assess its necessity and proportionality.

Wherever a policy, project, system, process or initiative includes the processing of personal data, that processing must be compliant with data protection legislation at the point of delivery. Completing a DPIA will help to assess whether the proposed data processing delivers 'Privacy by Design and by Default' in compliance with data protection legislation. DPIAs also contribute to the requirement to keep records of personal data processing activities.

Police Scotland's Information Assurance team have responsibility for managing DPIAs in Police Scotland and they, along with the Strategic Information Asset Owner, must approve a DPIA before any personal data can be processed.

Equality and Human Rights Impact Assessment

Although an Equality and Human Rights Impact Assessment (EqHRIA) is not an explicit requirement of equality or human rights law they are a key way to understand and help mitigate any potential equality or human rights harm that may come from the deployment of data or data driven technology

An EqHRIA is designed to help those developing a project consider the context within which it will operate from the outset and engage directly with those people identified whose rights may be at risk. It is designed to complement other impact and due diligence assessments and is framed by equality law and international human rights principles and conventions.

Community Impact Assessment

As per the College of Policing', 'the purpose of a community impact assessment (CIA) is to identify issues that may affect a community's confidence in the ability of the police to respond effectively to their needs, thereby enhancing the police response. It helps to inform forces about long-term plans to rebuild community confidence and learn lessons for the future. CIAs should be carried out efficiently and should accurately record the effect the incident has had on the community. When asking for a CIA, the following should be considered:

- what information is required and what it will be used for
- who can provide the information required and who will oversee the work
- how long it will take to complete.

[18] https://ico.org.uk/for-organisations/toolkit-for-organisations-considering-using-data-analytics/

An effective CIA may also:

- provide enhanced investigative assessment and an understanding of all aspects of the incident being dealt with
- identify vulnerable individuals and groups
- provide an assessment of community confidence in police response
- develop community intelligence.’