| Police Scotland logo | Freedom of Information ResponseOur reference: FOI 24-0223Responded to: 3rd June 2024 |
| --- | --- |

Your recent request for information is replicated below, together with our response.

## Please provide the following:Current Use of Artificial Intelligence:1. Is  Police Scotland  currently utilising any form of Artificial Intelligence or AI-driven technologies or services?1.1. If yes, in what capacities or areas are these AI technologies being used?

I can advise that Police Scotland in common with all other UK police forces, use Child Abuse Image Database (CAID) Retrospective Facial Recognition (RFR) functionality, the Police National Computer (PND) RFR functionality and Automatic Number Plate Recognition (ANPR) technology, all of which are managed and owned by the Home Office.

* PND collates images taken in custody and can provide a potential match to subject on images, captured during crimes. PND RFR is proven technology and an extremely useful tool in helping officers to identify those who commit crimes.
* CAID contributes to the fight against Online Child Sexual Abuse and Exploitation (OCSAE). It helps identify and safeguard victims, makes investigating Child Sexual Exploitation and Abuse faster and more effective and supports international effort to remove images from the internet. RFR seeks to automatically identify if the image of a person is present within the database, when uploaded by a law enforcement agency. CAID also has an Image Classifier software add-on which helps investigators sift and group images with the aim of quickly identifying Indecent Images of Children (IIOC). The software IT does not make decisions, but helps investigators review the images which are likely to be the highest priority first.
* ANPR is a system capable of reading vehicle number plates, used by policy to track down criminal behaviour and is also seen on many UK motorways as a method of detecting speeding through average speed calculation.
* Other UK policing solutions that have been used for over 20 years, are IDENT1 (national Fingerprint Database) or National DNA Database, that automate the search and comparison elements via Home Office approved algorithms. Any potential matches to be used for investigation purposes, are verified (or not) by a human (forensic scientist).

**Reports and Research:**
2. Has Police Scotland conducted, commissioned, or been provided with any reports or studies regarding the potential uses or implications of Artificial Intelligence within its operations?

## 2.1 If such reports or research exist, please provide copies or summaries of these documents.

In response to the two questions above I can advise that, Police Scotland’s Cyber Strategy 2020 ‘*Keeping People Safe in a Digital World’* was approved by the Scottish Police Authority (SPA) on 30 September 2020.  The Policing in a Digital World Program (PDWP) has a clear aim to transform how Police Scotland respond to the evolving threat of cybercrime to continue keeping Scotland’s people, communities, businesses, and assets safe in both the physical and virtual world. By ensuring all officers and staff on the frontline and in specialist roles have the knowledge, skills, tools, and support to confidently and effectively tackle cybercrime Police Scotland will be better equipped to prevent, respond to, and investigate such crimes; we must build the workforce and tools to keep people safe in public, private and virtual spaces.

Police Scotland and the Scottish Police Authority’s joint vision is to deliver comprehensive change to become a centre of excellence in digital and cyber policing. The Scottish Police Authority is committed to supporting Police Scotland in building public trust through open and transparent discussion and engagement, promoting, and supporting the need to build effective preventative partnerships and secure additional investment.

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

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

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

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

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

Policing in a Digital World will continue to assess any new technological developments which have the ability to make investigations and examinations more efficient whilst maintaining our overarching aim of Keeping People Safe in the physical and digital world. All technologies are routed through the above pathway and triage with a realisation that policing cannot ignore advancements in technology can however they will not relinquish, but compliment, the requirement for human interaction to support investigations.

## 3. Is Police Scotland currently looking at ways Artificial Intelligence could be implemented?

Police Scotland is considering ways in which Artificial Intelligence (AI) could benefit policing and improve the service provided to the public. The speed and accuracy that AI could bring to police processes make it an attractive way to deliver an effective and efficient service. However, the application of AI can be contentious if not properly explored and consulted on.

Police Scotland are currently engaging both internally and externally with a number of partners including the National Police Chiefs' Council (NPCC), Scottish Police Authority (SPA) and Scottish Biometrics Commissioners with regards to the use of AI and the following aspects:

* Strategy & Policy
* Practical use of AI
* Assurance & Scrutiny

These have also formed the basis of previous Research and Evidence Forums facilitated by the SPA.

If you require any further assistance, please contact us quoting the reference above.

You can request a review of this response within the next 40 working days by email or by letter (Information Management - FOI, Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH). Requests must include the reason for your dissatisfaction.

If you remain dissatisfied following our review response, you can appeal to the Office of the Scottish Information Commissioner (OSIC) within 6 months - [online](http://www.itspublicknowledge.info/Appeal), by email or by letter (OSIC, Kinburn Castle, Doubledykes Road, St Andrews, KY16 9DS).

Following an OSIC appeal, you can appeal to the Court of Session on a point of law only.

This response will be added to our [Disclosure Log](http://www.scotland.police.uk/access-to-information/freedom-of-information/disclosure-log) in seven days' time.

Every effort has been taken to ensure our response is as accessible as possible. If you require this response to be provided in an alternative format, please let us know.