Police Scotland and Scottish Police Authority Forensic Services
Joint Biometrics Strategy
2025-30

Contents

Document Details	
Document Title	Police Scotland and Scottish Police Authority Forensic Services Joint Biometrics Strategy
Version	v1.1
Date of Issue	*Add date of issue here*
Status	DRAFT

Foreword from the Deputy Chief Constable, Police Scotland

As we look to the future the Police Scotland Joint Biometrics Strategy plays a vital role in delivering our 2030 vision for policing in Scotland — a vision that aspires to create safer communities, reduce crime, and strengthen public trust in policing. Biometric technologies, when deployed responsibly, offer transformative opportunities for modern policing. From enhancing investigative capabilities to improving the speed and accuracy of identification, these tools are already supporting the vital work of officers and forensic services across Scotland.

However, with great capability comes great responsibility. This strategy is built on the firm foundation of Scotland's commitment to human rights, ethical oversight, and transparency. Our strategic objectives closely align to the Scottish Biometrics Commissioner's own strategic priorities, as outlined in his published Strategic Plan 2025-29 ensuring our use of biometric data is proportionate, lawful, and accountable. We are committed to regulatory compliance at every level and to fostering organisational awareness about the responsibilities and standards that govern biometric use. Maximising the benefits of technology requires more than investment in tools — it demands that we build and maintain the public's trust and confidence. This means placing privacy, equity, and fairness at the centre of everything we do. Our work with Forensic Services and regulatory partners ensures that biometric applications are grounded in scientific rigour, legal integrity, and operational necessity.

As we move toward 2030, this strategy will help guide how we responsibly and effectively use biometrics to prevent harm, protect the vulnerable, and build a Scotland where everyone feels safe and secure.

Foreword from Fiona Douglas, Director of Forensic Services

The Director of Forensic Services SPA reports to the Chair of the Scottish Police Authority. The SPA Forensic Services Committee, established in October 2018 by the Scottish Police Authority, provides oversight and scrutiny for the work of Forensic Services. One of the four Forensic Services strategic outcomes is that we work collaboratively with Police Scotland and other partners to serve the needs of the public and criminal justice in Scotland.

Our landscape is a rapidly changing and shifting environment where we are increasingly seeing new developments in both technology and science. Our other three strategic outcomes align and reference our people, services and resilience to future challenges.

Forensic Services strategic outcomes are the pillar of our organisation and we are cognisant that our current, and any future, processes have biometric and information data compliance as a cornerstone to everything we do. The majority of the processes conducted by Forensic Services are accredited to UKAS ISO 17025 which provides independent assurance for the technical competency, high standard of quality and impartiality of our processes provided to the Criminal Justice System.

By working with our Partners and the Scottish Biometrics Commissioner we will endeavour to be open, honest and transparent to ensure public trust and confidence in the use of biometrics, upholding individuals' rights while maintaining law and order to keep the public of Scotland safe.

Executive Summary

The responsible and ethical use of biometric data is a key priority for both Police Scotland and Scottish Police Authority Forensic Services as we seek to maximise public safety, while maintaining public trust and confidence within our communities. The strategy has a clear vision for the future strengthening of policing with new technologies, however, their use must be underpinned by clear principles of legality, necessity, proportionality and transparency. Advances in biometric technology, including DNA, fingerprints and facial matching offer significant opportunities to prevent and detect crime more efficiently. Other biometric data i.e. from CCTV recordings, Body Worn Video, Video Identification Parade Electronic Recording (VIPER), drones, digital forensics, recovered evidence (including the Digital Evidence Sharing Capability - DESC) will be governed to the same standard.

This strategy defines Police Scotland and Scottish Police Authority Forensic Services' approach to the collection, retention and use of biometric data to ensure compliance with legal and regulatory frameworks, including the Scottish Biometrics Commissioner's Code of Practice. Significant progress has been made and this strategy is intended to complement and support Police Scotland's Policing 2030 vision, the Joint Strategy for Policing (2023/26) and the Scottish Police Authority's Forensic Services Strategy. The strategy outlines future measures to strengthen governance, enhance engagement, improve oversight and ensure biometric technologies are deployed in a way that respects individual rights and privacy. This strategy covers both physical biometric samples as well as the data derived therefrom.

By working with key stakeholders, such as the Scottish Biometrics Commissioner, Information Commissioners Office and Scottish Government there is assurance of independent scrutiny and our clear commitment to best practice. Working jointly, we will continue to lead in the responsible and strengthened use of biometric data to support public protection and justice. We will use an open approach, seeking views and engagement from partners to inform and adapt the strategic roadmap with regular reviews auditable at executive level. Full access and transparency are assured for any external audit/auditor to maximise the potential for any unrecognised risks to be identified and to provide confidence both internally and externally to evidence compliance. Any recommendations for improvement may require prioritisation due to resource and financial challenges across both organisations.

Equally future developments with technological advancements, such as Live Facial Recognition, and updates to sharing agreements between police forces and government agencies will be acted upon through policy setting and organisational agreement.

Key Stakeholders

Plan on a page

Joint Biometrics Strategic Plan

Vision

To collect and use biometric data in policing in an ethical, lawful and transparent manner. To ensure public trust and confidence in the use of biometrics, upholding individuals' rights while maintaining law and order to keep the public of Scotland safe.

Aim

Drive change through continuous improvement, regulatory assurance and improving organisational awareness. Ensure horizon scanning to maximise our responsible use of biometric data and technological advances to keep our communities safe from harm whilst maintaining or enhancing public trust and confidence in the legitimacy of our approach.

Strategic Outcomes

Regulatory Compliance

Ensure compliance with legal requirements and policy principles to mitigate risk and maintain organisational integrity

Organisational Awareness

Promote understanding and compliance with the Scottish Biometrics Commissioner's Code of Practice to ensure lawful, ethical and effective practice

Maximising Technology

Leverage advancing technology to enhance public safety, support pro-active law enforcement and increase efficiency

Public Trust and Confidence

Ensure the public understand the need for biometric data, how it is retained, used and weeded from our systems

Policy and Legal Framework

Police Scotland and Scottish Police Authority Forensic Services will collect, use and retain biometric data for use in law enforcement to keep the public of Scotland safe from harm. In addition to the Scottish Biometrics Commissioner's Code of Practice, specific statutory legislation exists providing Police Scotland the authority to take, use and retain fingerprints and DNA data and physical samples from arrested persons, registered sex offenders and volunteers.

Where there are gaps in legislation, or where legislation is silent, samples and data are managed as per Police Scotland and Scottish Police Authority Forensic Services policy. There is a lack of primary legislation underpinning the acquisition, retention, sharing, use and weeding of facial images, however Scottish Government have committed to reviewing this in the future in line with the increasing availability of facial matching technologies.

There is awareness of human rights obligations and the broader impact of any wider UK or EU rulings. Under UK Data Protection law, biometric data is defined as 'special category data' due to its extremely sensitive nature and the important privacy, ethical and human rights considerations arising from its processing.

All biometric data will be legally held and controlled according to relevant legislation:

- Scottish Biometrics Commissioner Act 2020
- Scottish Biometrics Commissioner Code of Practice - November 2022
- Custody & Registered Sex Offenders Samples & Data (Section 18-19C) - Criminal Procedure (Scotland) Act 1995
- Volunteer Samples & Data (Section 56) - Criminal Justice (Scotland) Act 2003
- Data Protection - Data Protection Act 2018
- ECHR Gaughran Ruling (No indefinite retention without periodic review) - GAUGHRAN v. THE UNITED KINGDOM (UK)

- UK General Data Protection Regulation (UK GDPR)
- Age of Criminal Responsibility(Scotland) Act 2019 (Part 4, Chapter 4)

Biometrics used in Policing

Biometric data is integral to policing, to uphold the law, prevent crime and disorder, protect and reassure communities in the investigation of crime and support the criminal Justice system for the public of Scotland.

Biometric data is used to verify the identity of a person, to assist in eliminating a person as a suspect, to identify the source of evidence as part of a criminal investigation and to establish links across offences. Biometric data relates to human identification information that is formed following specific technical processing. Biometric data can be searched and compared to establish characteristics of 'uniqueness'.

Section 34 of Scottish Biometric Commissioners Act 2000 provides a definition of biometric data and samples used for policing purposes in Scotland.

"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 to establish the identity of an individual……..Physical data comprising or derived from a print or impression of or taken from an individual's body, a photograph or other recording of an individual's body or any part of an individual's body, Samples of or taken from any part of an individual's body from which information can be derived, and Information derived from such samples."

DNA

Acquisition

Taken from arrested persons, Registered Sex Offenders (RSOs), volunteers and complainers to determine their DNA profile for use as part of a criminal investigation and/or proceedings. Samples from staff, Police Officers and other laboratory visitors are also taken to ensure that inadvertent contamination events are robustly investigated to ensure the integrity of the casework result.

Use

For comparison to DNA data derived from materials left at crime scenes and other subject DNA data, to support the investigation of non-crime related incidents such as deceased or missing persons. Prior to results being used robust checks are undertaken to establish it meets the legal framework and retention rules.

Retention

Arrestee DNA profiles are routinely stored and shared locally, nationally and internationally with specific EU member states. Other DNA profiles are shared nationally or internationally if there is a justifiable policing purpose. The main conduits for DNA data retention are the Scottish DNA Database, owned by Scottish Police Authority Forensics Services, the UK National DNA Database owned and operated by the Home Office Forensic Information Databases and the Trade Cooperation Agreement EU Member Sharing DNA Database overseen by the Metropolitan Police.

Images

Acquisition

Captured from arrested persons, Registered Sex Offenders (RSO), volunteers and complainers for use as part of a criminal investigation and/or proceedings. Images are also captured by Scottish Police Authority Forensic Services Scene Examiners during their scene duties, when taking injury photographs (from injured parties; both complainers and suspects) or at the mortuary when taking photographs of a deceased person.

Use

For policing identification, including via facial matching, CCTV, identification parades, digital forensics purposes (e.g. mobile phones, ring doorbells, personal CCTV / security footage, dash-cams, etc.). Prior to results being used robust checks are undertaken to establish it meets the legal framework and retention rules.

Retention

Routinely stored and shared locally and nationally. If there is genuine and justifiable policing purpose it can be shared internationally. The main conduits for image retention are the Forensic Services Image Management System, Police Scotland Scottish Criminal History System and UK Police National Database owned and operated by the Home Office.

Fingerprints

Acquisition

Taken from arrested persons, Registered Sex Offenders (RSO), volunteers and complainers for use as part of a criminal investigation and/or proceedings. Elimination prints are sought from all Police Officers and staff who have cause to handle evidence to ensure the integrity of any identification. Immigration prints are taken as required.

Use

For comparison to fingerprint data derived from marks left at crime scenes and other subject fingerprint data, to support the investigation of non-crime related incidents such as disaster victim identification or missing persons. Prior to results being used robust checks are undertaken to establish it meets the legal framework and retention rules.

Retention

Routinely stored and shared locally and nationally. If there is genuine and justifiable policing purpose it can be shared internationally.   The main conduit for fingerprint data retention is the UK National Fingerprint Database which also facilitates Trade Cooperation Agreement EU Member Sharing, owned and operated by the Home Office Forensic Information Databases.

Biometric weeding

All data and physical samples stored in biometric databases are destroyed in accordance with legislative and policy requirements. Both Police Scotland and Scottish Police Authority Forensic Services have embedded extensive governance activities to ensure compliance in this space.

Strategic Outcomes

1. Regulatory Compliance

Objective: We aim to ensure compliance with biometric regulations and to maintain the integrity of our operations. Adhering to the principles set out by the Code of Practice ensures that the collection, retention and use of biometric data – such as fingerprints, DNA and facial images – are necessary, conducted lawfully, ethically and proportionally safeguarding an individual's right to privacy.

We will:

- Improve retention policy where legislation is silent, including periodic review to align with data protection requirements.
- Consider aligning image retention, as closely as possible, to DNA and Fingerprints taken for the same arrest incident.
- Review the requirement to maintain and use > 1.1 million hard copy fingerprint records in addition to electronic held records (Risk -v- benefit -v- cost analysis)
- Seek technical solutions for biometrics systems with limited/lacking weeding capacity.
- Seek technical solutions for biometrics systems with limited audit and logging facilities.
- Review and improve the end-to-end management of volunteer data and samples, including consent recording and sharing protocols.
- Review the use of current internal auditing resource to potentially supplement any external audit plan.
- Comply with the data-sharing requirements of international policing, including the upcoming new provisions under Prum 2.

2. Organisational Awareness

Objective: We aim to embed regulatory requirements into operational policy, guidance and procedures, and to provide ongoing training to staff, demonstrating our commitment to responsible data management and adherence to the highest standards of human rights and ethical policing.

We will:

- Identify opportunities for bespoke biometric training for police officers and relevant staff.
- Increase awareness of Scottish Biometrics Commissioner Code of Practice obligations across both organisations.
- Refresh and maintain the contents of the joint Biometrics Acquisition (DNA, Fingerprints and Facial Images) Standard Operating Procedure.
- Develop national biometrics guidance documentation to complement existing operating instructions.
- Consider dedicated biometric intranet pages, or hubs, to streamline information and support for officers and staff.

3. Maximising Technology

Objective:

We aim to leverage advancing biometric technology to enhance public safety, improve investigative capabilities and ensure the effective administration of justice.

As crime becomes increasingly complex and technologically sophisticated, the use of biometric tools is essential in delivering accurate and timely results. Maximising these technologies allows us to provide biometric matches more efficiently.

However, the adoption of biometric technology must be balanced with ethical considerations, legal compliance and public trust. By investing in advancing biometric solutions, while ensuring transparency and accountability, we can strengthen its operational effectiveness and uphold the rights and privacy of the communities it serves.

We will:

- Progress national conversations and considerations in respect of advancing facial matching capabilities.
- Improve the quality of images captured in custody to support emerging facial matching technologies. As a consequence of new technologies review the weeding and retention as appropriate.
- During the replacement of the current DNA robots explore more efficient and enhanced automation for extraction procedures.
- Review the future of advanced sequencing ability to aid analysis.
- Improve the processes within fingerprints to develop a paperless approach and progress new technologies when appropriate such as a digital workflow which will streamline process.
- Engage with UK forces and international law enforcement agencies to identify opportunities for wider sharing and use of multi-agency biometric technology.

- Improve Scottish biometric platforms, reviewing opportunities for automated weeding of data and interfaces with other UK biometric databases.
- Improve data availability and quality levels of biometric data to ensure maximum benefit (Risk -v- benefit -v- cost analysis).

4. Public Trust and Confidence

Objective:

We aim to enhance public trust and confidence in the use of biometrics and are committed to transparency, accountability, and proportionality being embedded in all biometric data practices.   This includes clear articulation of policy, retention periods, legal frameworks, ethical standards, and addressing public concerns.

Regular publication of statistics on biometric data use, retention, and deletion will provide reassurance that data is handled responsibly.

Engaging with stakeholders, including the Scottish Biometrics Commissioner, human rights groups and the public will foster a collaborative approach to policy development. Additionally, independent oversight and robust governance measures will strengthen our commitment to best practice. We will communicate clearly about what these measures are and how the public and stakeholders can find information.

We will:

- Consider requirement to utilise our in-house Research and Insight team to design public consultation and engagement when relevant in respect of biometric data or new technology.
- Utilise the findings from the Independent Advisory Group on Emergency Technology in Policing report, ensuring that the implementation of any new biometric technology use is aligned to these recommendations.

17

- Review improvements to existing quarterly published biometrics information.
- Introduce a joint Biometrics Annual Report to provide more detailed information not routinely reported.
- Compile and detail joint responsibilities across the acquisition, retention, sharing, use and weeding of biometrics, locally, nationally and internationally.
- Seek technical solutions for biometrics systems with limited / lacking management information reporting capabilities.
- Review the Biometrics Leaflet provided to the public which will inform the creation of similar leaflet for volunteers / complainers.
- Expand the contents of the Police Scotland Records Retention SOP to include other biometric data.
- Support external scrutiny assessments, and where relevant, comply with external scrutiny recommendations.

Governance & Accountability

Governance and accountability are the responsibility of the Chief Constable and the Director of Forensic Services. Both Police Scotland and Scottish Police Authority Forensic Services have embedded a biometrics governance and accountability structure within their senior leadership team.

The Assistant Chief Constable for Major Crime, Public Protection and Local Crime is the Police Scotland Biometric Data Owner. Police Scotland have introduced a dedicated biometrics portfolio to promote best practice, co-ordinate audit and recommendation activity, oversee data governance and quality assurance activity, whilst providing subject matter advice and support to officers, staff and stakeholders.

SPA Forensic Services have senior managers and subject experts as part of a strategic and tactical approach to promote and support governance activity across biometric data and systems. Scottish Police Authority Forensic Services are seeking to review the use of current internal auditing resource to potentially supplement any external audit plan. This will strengthen the audit program to ensure effective compliance with legislation and the Biometric Commissioner's expectations.

Biometric Risk Registers have been established within both organisations. These are reviewed separately, and jointly, at regular intervals by the portfolio holders and subject experts including Audit and Risk Leads and Information Security Management. This provides assurance that emerging risks are captured and assessed together with established risks to minimise, monitor and control the probability of those risks occurring.

Full access and transparency are assured for any internal or external audit to maximise the potential for any emerging risks to be identified and considered within the risk register process.

The Police Scotland Biometrics Oversight Board, with members from SPA, Forensic Services, the Scottish Biometrics Commissioner's office and Scottish Government, governs the strategic oversight, decision making and risk management in respect of biometric data and samples.   Strategic priorities and external scrutiny recommendation progress is monitored and measured at this Board and other executive committees, including the public Scottish Police Authority Policing and Performance Committee.

New proposals for data-driven technologies are subject to a robust review under the Rights Based Pathway, which ensures proposals are reviewed with an ethical lens, and where appropriate escalated for additional scrutiny and mandatory consultation. Where relevant, proposals are escalated to the Data Ethics Oversight Group providing a further level of audit and assurance encompassing ethical considerations.

To ensure a joined-up approach to data flow between police investigations and forensic scientific expertise, meeting the needs of our criminal justice partners locally, across the UK and internationally, Police Scotland and Scottish Police Authority Forensic Services work closely with stakeholders such as the Home Office, NPCC and NCA via established partnership boards. This provides confidence that Scottish data being used by other Law Enforcement Agencies, meet the standards and lawful requirements under Scottish law and policing policy.

Useful Resources

Police Scotland 2030 vision for policing.

Our 2030 vision and three-year plan

Forensic Services Strategy for 2025 - 30

https://www.spa.police.uk/spa-media/vohdf4d4/forensic-services-strategy-2025-2030.pdf

Police Scotland links to biometric information (including Custody Biometrics Management Information)

www.scotland.police.uk/access-to-information/biometrics/

www.scotland.police.uk/access-to-information/policies-and-procedures/

www.scotland.police.uk/access-to-information/data-protection

SPA Forensic Services website

Forensic Services | Scottish Police Authority

Scottish Biometrics Commissioner website which includes access to their codes of practice

www.biometricscommissioner.scot

Information Commissioner's Office website

https://ico.org.uk/