

Meeting	Forensic Services Committee
Date	8 August 2022
Location	Microsoft Teams
Title of Paper	Biometrics Landscape and Governance update
Presented By	Fiona Douglas
Recommendation to Members	For Noting
Appendix Attached	No

PURPOSE

This paper sets out the current position to consolidate the SPA FS Biometrics Strategy. The current primary focus relates to Fingerprints and DNA -biometric samples with which SPA FS has direct engagement. This paper covers:

- Key principles of our SPA FS Biometric Strategy
- Police Scotland Approach – SPA FS Integration
- Home Office – SPA FS Collaboration
- SPA FS Biometrics Working Group

1. BACKGROUND

- 1.1 Biometric samples are powerful investigative tools which can help enquiries exclude people, inform investigative lines, as well as ultimately provide compelling evidence in court proceedings.
- 1.2 The acquisition, retention, and weeding of samples and relevant physical data in Scotland are governed by the Criminal Procedure (Scotland) Act 1995 and Section 18 sets out the provisions which must be adhered to when taking, using, and weeding biometric samples.
- 1.3 The primary focus of the SPA FS Biometrics Strategy are those biometric samples with which SPA FS has direct engagement – Fingerprints and DNA - and particularly how we manage data exchange relationships with UK and international databases.
- 1.4 **Fingerprints:** Forensic Services currently operate Scotland's digital fingerprint collection of arrested/convicted people as part of a fully-integrated collection with England, Wales and Northern Ireland on IDENT1. While this offers advantages in the identification of marks in cross border crimes such as drugs cases, Scotland has faced considerable challenges in delivering legislative compliance for retention of our biometric fingerprint data.
- 1.5 **DNA:** SPA Forensic Service maintains the Scottish DNA database - established in 1996 - which contains DNA profiles obtained by the criminal justice process in Scotland. The Scottish DNA Database is maintained by a private contractor and our independent control of Scottish DNA data allows it to be maintained and updated in line with Scottish legislative requirements. An encrypted data transfer arrangement is used to link Scottish profiles with the UK DNA database.
- 1.6 SPA Forensic Services regularly publish statistics on the SPA website relating to the Scottish DNA Database (- [Scottish Police Authority \(spa.police.uk\)](https://www.scottishpolice.uk)). This includes the number of profiles held on the database, the number of profiles added and removed and those successfully matched along with information on the DNA profiles profiled from samples recovered at scenes of crime.

2 Key Principles of our SPA FS Biometrics Strategy

OFFICIAL

- 2.1 SPA FS are accountable for ensuring individual biometric data is used in a manner, which is ethically responsible, legislatively compliant and respectful of the rights of individuals, whilst at the same time facilitating its use in the investigation and resolution of crime.
- 2.2 Our Biometric Strategy is informed by the governing principles and ethical considerations as defined in section 5 of the Independent Advisory Group on the Use of Biometric Data in Scotland's report, published March 2018. Our use of biometric technologies and forensic procedures should;
- enhance public safety and the public good;
 - advance the interests of justice;
 - respect human rights of individuals and groups;
 - respect the dignity of all individuals;
 - take particular account of the rights of children;
 - take particular account of the rights of other vulnerable groups and individuals;
 - protect the right to respect for private and family life;
 - scientific and technological developments be harnessed to promote the swift exoneration of the innocent, afford protection and resolution for victims, and assist the criminal justice process;
 - be based on validated evidence
- 2.3 In the specific context of implementation with regard to the collection and processing of data the governing principles should be applied as follows;
- data should be collected, stored, used and retained only for specified and lawful purposes;
 - data collection, storage, and use must adhere to legal requirements;
 - steps should be taken to ensure the accuracy, security and integrity of data collected, stored and used;
 - steps should be taken to ensure transparency around error rates and uncertainties inherent in the procedures;
 - processes should be robust and conform to any relevant standards and be applied by professionally trained staff whose work can be audited;
 - intrusion into private lives should be minimised – this may be of particular significance in relation to issues of data linkage;
 - account should be taken of the interests of secondary data subjects (i.e. people potentially affected by data collected from others, e.g. family members);

OFFICIAL

- policies should be in place around the weeding and disposal of these data, including a presumption in favour of deletion.
- 2.4 Our strategy is focused on achieving effective and efficient Scottish control of Scottish biometrics data in all key touchpoints and data exchange systems, fully aligned to the governing principles as defined about and with appropriate frameworks in place to comply with the application requirements.
- 2.5 It is critical that we continue collaborative working strategies with our criminal justice partners, Police Scotland and Home Office Biometric Programme (HOB), as we seek to align our SPA FS Biometric Strategy with the strategy of Police Scotland and the UK Biometric Strategy being progressed by the UK National Police Crime Committee (NPCC).
- 2.6 We also continue to engage with the Scottish Biometric Commissioner to ensure we contribute to and ultimately comply with the codes of practice and regulations emerging from the commissioner's office.

Police Scotland Approach

- 2.7 SPA FS are fully engaged with Police Scotland, who have now established a robust data governance structure through the work of the Chief Data Office which provides data governance, lifetime management of National Systems, information assurance, disclosure, guidance and support across the Police Scotland data estate, embedding data ownership across the business.
- 2.8 The Chief Data Office provides the following services and we continue to engage in this activity as appropriate through our established representation on both the Biometrics Oversight Board and the Biometrics Data Owner Group.
- Data Architecture & Modelling
 - Data Breaches
 - Data Standards & Catalogues
 - Data Ethics
 - Liaison with the Information Commissioner's office
 - Individual Rights Requests
 - Information Assets Register
 - Data Quality
 - Lifetime Management
 - Records Management

OFFICIAL

- Data Protection Impact Assessments

2.9 Forensic Services are represented at both the Police Scotland Biometrics Oversight Board and the Biometrics Data Owner group providing appropriate updates on our biometric risk mitigation activity. The board's macro-level action plan has adopted a data asset ownership approach which is best managed within existing structures with the required tactical expertise.

2.10 The Director of Forensic Services, sits on the Police Scotland Biometrics Oversight Board, which is chaired by an ACC Lead in this area. A FS Head of Function Lead and an Operations Manager Expert Lead attend the Biometrics Data Owners Group. The Operations Manager Lead along with the SPA Audit and Risk Lead also meet with PS colleagues to review in detail our respective biometrics risk registers.

Home Office – SPA FS Collaboration

2.11 SPA FS works in partnership with the Home Office Biometric Programme covering both the UK fingerprint database (IDENT1) and the UK DNA Database (NDNAD).

2.12 While the data exchange mechanism for DNA currently works well, the management of legislative compliance of Scottish Data on the NDNAD is an intensive manual-based process which does not deliver the efficiencies of automated electronic data transfer

2.13 The 2003/2004 Scottish Government decision to amalgamate with IDENT1, was made at a point when the design build for the system was almost complete. Ad-hoc data exchange arrangements were put in place to facilitate the exchange of record management data between PNC and our own data control mechanism, the Scottish Criminal History System (CHS). While these mechanisms are electronic they do not provide the level of data control required. Manual work-arounds and resource-intensive reconciliation processes have prevented Scotland from accessing the range of business benefits associated with IDENT1 that are enjoyed by our UK Colleagues.

2.14 In June 2020 an extensive report ***Home Office Biometrics Programme: Implications and future options for biometric data and biometric policing databases in Scotland*** was

OFFICIAL

submitted to the SPA Forensic Services Committee and Scottish Government.

- 2.15 Principal among the report's recommendations is that, in contributing to wider UK policing databases, Police Scotland and SPA Forensic Service should ensure that they have the functionality to administer and maintain Scottish biometric data in accordance with Scottish legislation, Scottish policing policy, and any Codes of Practice in terms of its use.
- 2.16 The ultimate aim is for Scotland to have the capacity to independently manage Scottish data on UK databases. Through establishing appropriate electronic interfaces with our primary case recording system (CHS) we should then be able to fully align with the functionality available to UK colleagues. The challenge is to determine how/if this can be accommodated within the scope of the current HOB programme without additional overheads being remitted to Police Scotland/SPA/Scottish Government.
- 2.17 Work continues to upgrade/replace the Scottish DNA database and investigation of an appropriate electronic data exchange solution will be explored as part of the technical architecture.
- 2.18 There has been engagement for a number of years with HOB and PNC to deliver on Scottish Strategic requirements for IDENT1. HOB have been supportive in principle but it has been challenging to identify the resource required for a clearly defined bespoke plan of action to address Scottish requirements. HOB have identified a single point of contact at tactical level and this lead has been working with the Fingerprint Operations Manager to deliver on previously submitted service change requests and there has been some progress at this level.
- 2.19 A key element of our Biometric Strategy is to work within existing systems to deliver greater independent control of Scottish biometric data on national systems. To this end we have been seeking enhanced PNC permissions for nominated SPA FS fingerprint staff to facilitate the timely weeding of Scottish fingerprint records from the UK fingerprint database – IDENT1. This was an unprecedented request, which required direct engagement at PNC executive level over a prolonged period of time, however agreement was secured, the technical design agreed and we have now embarked on the testing and monitoring phase prior to implementation Q4 2022/23. Securing of these enhanced permissions will transform our ability to

OFFICIAL

directly control Scottish data on UK systems and provide the platform needed to move forward to our longer term aim of CHS integration with UK biometric databases.

- 2.20 There is also a more comprehensive schedule of work that is also taking place with the Home Office - The Law Enforcement Data Service (LEDS) which is the development of a modern cloud-based data service that will enable the future retirement of the Police National Computer (PNC). Police Scotland are fully engaged with the Home Office regarding this project and SPA Forensic Services are also supporting. This is to ensure there is a wider strategic solution to incorporate Scotland's requirements relating to the use of IDENT1 and especially given the primacy of CHS and avoid a situation that occurred back in 2003/2004.

SPA FS Biometrics Working Group

- 2.21 SPA FS Senior Management Team have established a SPA FS Biometrics Working Group to;

"Provide strategic direction and oversight of all matters pertaining to "biometric data" which influences and impacts Forensic Services. The Board will ensure that Forensic Services comply with the law and transparently uphold the rights of all citizens in Scotland".

- 2.22 Specifically the working group will;

- Create a well-informed strategic and cohesive approach to biometrics across Forensic Services.
- Provide liaison and support for the Scottish Biometrics Commissioner ensuring that their work is supported across Forensic Services, including engagement in the creation of, and adherence to a Code of Practice and legal changes
- Provide high level oversight of compliance with the statutory Code of Practice under the Scottish Biometrics Commissioner Act 2020, including collaborative working and shared good practice with other public bodies and partner agencies.
- Facilitate the coordination of all areas of Forensic Services to ensure compliance to coherent, consistent, justifiable, lawful and ethical policies which directly relate to biometric data or impact on biometric data in relation to obtaining, retaining, using and deletion of said data.

OFFICIAL

- Monitor and influence investment priorities to ensure they are aligned with strategic priorities for Forensic Services.
- Provide strategic leadership in relation to future and emerging technologies, and legislation provide advice / recommendations to the Force Executive in relation to any future use of such technologies in Scotland, including learning from UK-wide participation on the Home Office Biometrics Board.
- Develop an internal and external Communications Plan.
- To ensure the Risks are clearly understood and mitigated.

2.23 The working group is chaired by the Head of Function Lead supported by the Operations Manager Expert Lead, with representation from relevant business areas, Police Scotland colleagues and SPA Corporate. Output to date:

- Identification of data categories
- Collation of single suite of biometrics documents jointly owned by SPA & Police documents which clearly define the acquisition, use, management, retention and disposal of biometric data across both organisations
- Biometric data mapping exercise tracking the journey of our biometric physical samples (fingerprints & DNA), across our business areas within the context of the data governing principles and legislative compliance.
- Identification of key risk areas, collation of our SPA FS Biometric Risk Register.

Work in progress within the group is the population of the Biometrics Strategic Road Map with assigned action owners and timeframes for delivery as part of our data risk mitigation.

3. FINANCIAL IMPLICATIONS

3.1 There are no direct financial implications in this report.

4. PERSONNEL IMPLICATIONS

4.1 There are no personnel implications associated with this paper.

5. LEGAL IMPLICATIONS

5.1 There are no further legal implications in this paper to those listed above.

6. REPUTATIONAL IMPLICATIONS

6.1 There are no reputational implications associated with this paper.

7. SOCIAL IMPLICATIONS

7.1 There are no social implications associated with this paper.

8. COMMUNITY IMPACT

8.1 There are no community implications associated with this paper.

9. EQUALITIES IMPLICATIONS

9.1 There are no equality implications associated with this paper.

10. ENVIRONMENT IMPLICATIONS

10.1 There are no environmental implications associated with this paper.

RECOMMENDATIONS

Members are requested to:

Note the information contained within this report.