SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Agenda Item 7

Meeting	**Authority Meeting**
Date	**24 November 2022**
Location	**COSLA, Edinburgh**
Title of Paper	**Scottish Biometrics Commissioner Code of Practice and Compliance**
Presented By	**Brian Plastow (Scottish Biometrics Commissioner)** **Fiona Douglas (Director Forensic Services)** **Deputy Chief Constable Malcolm Graham**
Recommendation to Members	**For Discussion**
Appendix Attached	**Yes** **Appendix A - Code of Practice – Scottish Biometrics Commissioner**

PURPOSE

The purpose of this paper is to update Members on the Scottish Biometrics Commissioner's recently published Code of Practice and the Annual Report and Accounts.

The paper also seeks to update the Authority on Police Scotland and Forensic Services compliance with the Code.

1 Background

1.1. The Scottish Biometrics Commissioner Act 2020 was passed by the Scottish Parliament on 10 March 2020 and received Royal Assent on 20 April 2020. The Act established the office of Scottish Biometrics Commissioner and provides for its functions.

1.2. The Commissioner is independent of Scottish Government and is appointed by His Majesty the King on the nomination of the Scottish Parliament. The Commissioner's general function is to support and promote the adoption of lawful, effective, and ethical practices in relation to the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes by Police Scotland, the Scottish Police Authority (SPA), and the Police Investigations and Review Commissioner (PIRC).

1.3. 'Biometric data' means 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. Biometric data may include:

a. Physical data comprising or derived from a print or impression of or taken from an individual's body,

b. A photograph or other recording of an individual's body or any part of an individual's body,

c. Samples of or taken from any part of an individual's body from which information can be derived, and

d. Information derived from such samples.

1.4. The Biometrics Commissioner laid his first ever Annual Report and Accounts (ARA) in front of Scottish Parliament on the 25th October and the Scottish Biometrics Commissioner Code of Practice (CoP) will come into force in November 2022.

1.5. This paper seeks to summarise key points from the ARA and update members on the recently published CoP. It further seeks to update the Authority on Police Scotland and Forensic Services' compliance with the CoP.

2 Scottish Biometrics Commissioner Annual Report and Accounts

2.1. The ARA gives a sense of scale in terms of biometrics data collection for criminal justice and policing purposes in Scotland. It states that over 640,010 images of 374,405 individuals are held on Police Scotland Criminal History System and UK Police National Database. Over 1,000,000 other images are held for policing and criminal justice purposes with no automated biometric searching capabilities.

2.2. In terms of DNA profiles 383,279 DNA Profiles exists with 19,845 unmatched Crime Scene DNA Profiles. Policing in Scotland also hold 739,408 fingerprints relating to 412,127 individuals.

2.3. The ARA notes that biometric data for policing and criminal justice purposes makes a valuable contribution to public safety in Scotland and the Commissioner concludes that the Scottish Parliament should have confidence in the ways in which biometric data and technologies are currently being used by Police Scotland, the SPA and PIRC for policing and criminal justice purposes in Scotland.

2.4. The Biometrics Commissioner's ARA contains three recommendations made under section 32 (2) (c) of the Scottish Biometrics Commissioner Act 2020:

1. Scottish Government should progress a legal resolution to realign the provisions of Section 28(period of Strategic Plan) and Section 29 (budget period) of the Scottish Biometrics Commissioner Act 2020, in line with the original policy intention of the founding legislation.

2. If proceeding to implement any future expansion of the functions of the Scottish Biometrics Commissioner beyond Police Scotland, the Scottish Police Authority and the Police Investigations and Review Commissioner, Scottish Government and the Scottish Parliamentary Corporate Body should firstly consult with the Commissioner prior to producing a comprehensive business assessment of the likely impact on both the established function and personal responsibilities of the Commissioner.

3. In contributing biometric or forensic data to UK policing systems, Police Scotland and the Scottish Police Authority should ensure they have the functionality to

administer and maintain that Scottish data, in compliance with Scottish legislation and any Codes of Practice in terms of its use.

2.5. The ARA also contains several key findings that related to public confidence in biometrics and application of safeguards regarding new technology:

- There have been significant concerns about the use of biometric data in other public sector contexts in Scotland during 2021/22, but these have not extended to criminal justice or policing.

- The ARA highlighted that a public attitudes and awareness survey conducted for the Scottish Biometrics Commissioner (SBC) by ScotCen in December 2021 points to fairly high levels of public confidence in the use of biometrics for policing and criminal justice purposes in Scotland.

- Police Scotland has taken a measured approach to technologies involving 'face' and has not deployed overt live facial recognition technology in Scotland. However, there are circumstances where, with appropriate safeguards, such technologies could enhance public safety.

- Digital forensic techniques can recover biometric data that has the potential to enter the chain of evidence from crime scene to court. It is therefore essential that the processes and procedures underpinning such techniques are independently validated and accredited.

3 Code of Practice – Scottish Biometrics Commissioner

3.1. The Scottish Biometrics Commissioner's CoP came into effect in Novmber 2022. This Code seeks to promote good practice, transparency, and accountability in Scotland by setting out an agreed framework of standards for professional decision-making which strikes the right balance between the needs and responsibilities of policing and our criminal justice system. This gives consideration to enforcing the law and keeping citizens safe, and the fundamental obligation to guarantee the basic human rights, privacy, and freedoms of individual members of the public.

3.2. The CoP sets out that when acquiring, retaining, using, or destroying biometric data for criminal justice and policing purposes

in Scotland, Police Scotland, the SPA and PIRC must adhere to 12 General Guiding Principles and Ethical Considerations.

3.3. These Guiding Principles and Ethical Considerations are: Lawful authority and legal basis; Necessity; Proportionality; Enhance public safety and public good; Ethical behaviour; Respect for Human rights of individuals and groups; Justice and accountability; Encourage scientific and technolocial advancement; Protection of children, young people and vulnerable adults; Promoting privacy enhancing technology; and Retention periods authorised by law.

3.4. The guiding principles contained within the CoP also seek to provide a mechanism to Police Scotland and Forensic Services through which judgements can be formulated when considering the implementation of whether new biometric technologies should be implemented or not. The CoP also includes provision for the Scottish Biometrics Commissioner and the Commissioner's Advisory Group to independently offer ethical advice to Police Scotland, the Scottish Police Authority and Police Investigation and Complaints Commissioner on request when consdeiring new biometric technology or a new application of exitisting technology.

3.5. In terms of monitoring and reporting on the CoP, the Scottish Biometrics Commissioner must keep the approved Code of Practice under review, prepare and publish a report on the Commissioner's findings, and lay a copy of the report before the Scottish Parliament. The first report must be laid before the Parliament no later than three years after the date on which the first Code of Practice comes into effect. Subsequent reports must be laid before the Parliament no later than four years after the date on which the last such report was laid.

3.6. The Scottish Biometrics Commissioner also has a duty under Section 15 of the Act to provide a procedure by which an individual, or someone acting on an indviduals behalf, may make a complaint to the Commissioner that a person who is required to comply with the CoP has not done or is not doing so.

3.7. Section 27 of the Act provides that where a person to whom a compliance notice has been issued refuses or fails, without reasonable excuse, to comply with the notice, the Commissioner may report the matter to the Court of Session. After receiving such a report and hearing any evidence or representations on the matter, the Court may (either or both):

A. make such order for enforcementas it considers appropriate,

B. deal with the matter as if it were a contempt of court.

3.8. The CoP has been published as a draft on the Scottish Biometrics Commissioner's website since 2 September 2022. Work has been underway within Police Scotland and Forensic Services to ensure compliance with the CoP.

4 Police Scotland Update on the Code of Practice

4.1 Data Ownership

Police Scotland and Scottish Police Authority Forensic Services have a signed Joint Data Owner Agreement in respect of DNA and Fingerprint biometric data. Governance and oversight of data (including physical samples) is primarily shared as follows:

PS led:

- Arrestee Criminal Justice (CJ) DNA
- Arrestee Images
- Video (i.e. ViPER, Body Worn Cameras, CCTV, drones, etc.)

4.2 Data Governance Structure

Police Scotland implemented a new Biometrics governance structure in direct response to the Scottish Biometrics Commissioner Act 2020. ACC Bex Smith leads the executive Police Scotland Biometrics Oversight Board (BOB) attended by the Scottish Biometrics Commissioner, the remit of which extends to 4 portfolios:

- Biometric Data (ACC Spiers)
- Data Ethics (ACC Spiers)
- Technology / Futures (Andrew Hendry, Chief Digital and Information Officer)
- Forensic Science (Fiona Douglas, Director of SPA FS)

ACC Bex Smith is the Biometric Data (& Asset) Owner, leading the strategic Biometric Data Owner Group (Bio DOG), reporting directly to and supporting the BOB. Initial efforts have concentrated on "traditional" biometrics, namely Criminal Justice DNA and images from arrestees. Video data will be reviewed in due course.

The Data Owner is supported at tactical level via a delegate DCS and activity co-ordinated by the PS Biometric Data Steward. The Data Steward will identify and escalate Biometric Data risks via the Enterprise Data Risk Register (EDRR), ensuring Police Scotland Senior Information Risk Owner (SIRO) sight at the Data Governance

Board. Support is also provided by the Police Scotland Data Ethics Lead.

4.3 Arrestee Criminal Justice DNA Samples

DNA from Arrested persons is taken under and subject to the powers of S18-19C of the Criminal Procedure (Scotland) Act 1995 ('the 95 Act).

In 2021, Police Scotland completed a successful review of the full Criminal Justice data journey (Acquisition, Storage, Sharing, Use and Retention) the results of which allow confidence Police Scotland align to the Scottish Biometrics Comissioner, Code Of Practice as far as possible across Scottish, UK and International DNA databases.

4.4 Arrestee Images

Arrest images were highlighted as an area of concern in the 2018 Independent Advisory Group Report and through various engagement sessions with the Scottish Biometrics Comissioner. The same in-depth review of the data journey is in progress.

- Custody System(s)
  In August 2022, Police Sscotland weeded all images uploaded to the National Custody System (NCS) and disabled the ability for any to be added in the future.

- Criminal History System (CHS)
  CHS is the main conduit for arrestee image retention within Police Scotland. These Images also continue to be held on the Police National Database (PND). Work is also ongoing to introduce automated weeding to prevent the same risk materialising in the future.

- PND
  Police Scotland currently share all CHS arrestee images to PND and weeding of PND data is in tandem with CHS.

4.5 Data Ethics

Police Scotland aims to become an organisation 'driven by effective and efficient use of data in an ethical way'. To support this aim, a Data Ethics Strategy ('the Strategy') and Data Ethics Governance Framework ('the Framework') were developed in partnership with the UK Government's Centre for Data Ethics and Innovation (CDEI) and

ratified by Police Scotland's Senior Leadership Board in 2021. Once fully operationalised, the key components of the Data Ethics process will be a Data Ethics triage, the introduction of a new internal Data Ethics Oversight Group (DEOG) and an external Independent Data Ethics Group (IDEG).

The Chief Data Office's new Data Ethics function will support, rather than diminish, the role of Ethics Advisory Panels. Ethics Advisory Panels (EAPs) are a voluntary process to provide advice and support from Independent, National, Regional or Youth EAPs to anyone with an ethical dilemma that goes beyond normal and expected decision making. Dilemmas considered by the panels in the past include the Retention of Convicted Subject Biometric Data.

It is estimated these groups will be established late 2022 / early 2023, within initial focus on projects working with the Chief Data Office to assess the Data Ethics risk associated to their proposed use of data driven technology and for any projects identified as High Risk (and some others by exception) to be referred for further scrutiny.

5 Forensic Services Update on the Code of Practice

5.1. Forensic Services have established a Biometrics Working Group to oversee all casework and processes within the organisation relating to biometric samples with which SPA FS have direct engagement – Fingerprints and DNA - particularly how we manage data exchange relationships with UK and international databases.

5.2. Forensic Services are accountable for ensuring individual biometric data is used in a manner which is ethically responsible, legislatively compliant, and respects the rights of individuals, while at the same time facilitates its use in the investigation and resolution of crime.

5.3. The acquisition, retention, and weeding of samples and relevant physical data in Scotland are governed by the Criminal Procedure (Scotland) Act 1995; Section 18 sets out the provisions which must be adhered to when taking, using, and weeding biometric samples.

5.4. 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.

5.5. DNA: Forensic Services maintain 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.

5.6. Statistics are regularly published on the SPA website relating to the Scottish DNA Database. 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.

5.7. The Director of Forensic Services has made all members of staff aware of the Scottish Biometrics Commissioner's Code of Practice and their responsibilities to adhere to the code.

5.8. The strategic approach to Biometrics being taken by Forensic Services was reported into the SPA Forensic Services Committee in the Biometrics Landscape and Governance paper in August 2022.

6 FINANCIAL IMPLICATIONS

6.1. There are no financial implications in this report.

7 PERSONNEL IMPLICATIONS

7.1. There are no personnel implications in this report.

8 LEGAL IMPLICATIONS

8.1. There are no legal implications in this report.

9 REPUTATIONAL IMPLICATIONS

9.1. There are no reputational implications in this report.

10 SOCIAL IMPLICATIONS

10.1. There are no social implications in this report.

11 COMMUNITY IMPACT

11.1. There are no community implications in this report.

12 EQUALITIES IMPLICATIONS

12.1. There are no equality implications in this report.

13 ENVIRONMENT IMPLICATIONS

13.1. There are no environmental implications in this report.

RECOMMENDATIONS

Members are invited to note the Scottish Biometrics Commissioner's update on their Annual Report and Accounts and Code of Pracitce.

Members are asked to discuss Police Scotland and Forensic Services update on compliance with the Code of Practice.

Version 1.0 / November 2022

Code of Practice

On the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes in Scotland.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Safeguarding our biometric future

Approved by Scottish Ministers according to Section 12
of the Scottish Biometrics Commissioner Act 2020
Scottish Biometrics Commissioner November 2022.

www.biometricscommissioner.scot

Version 0.1 Reviewed by SBC Advisory Group established under Section 33 of the Scottish Biometrics Commissioner Act 2020. (01 July to 30 September 2021)	
Version 0.2 Reviewed by statutory consultees and others as considered necessary by the Commissioner under Section 10 of the Scottish Biometrics Commissioner Act 2020. (01 October to 31 December 2021)	
Version 0.3 Updated in January 2022 following 3-month closed consultation Amended by Dr Brian Plastow	Amendments made to previous version 0.2 • Minor proofing amendments to incorporate HMICS review and feedback • Minor observations from Forensic Science Regulator for England and Wales • Minor proofing matters from SG Police Division officials • Paragraph 47 expanded re feedback from Lord Advocate including referencing that the definition of biometric data in Scotland covers biological samples, including crime scene samples. Principle 12 also clarified re child offender legislation. • Minor amendments to principles 4, 5, 7 and 12 to reflect feedback from GeneWatch UK. • Minor amendments from the Equality and Human Rights Commission (EHRC) to add additional references to the Public Sector Equality Duty (PSED) and a hyperlink to the EHRC Equality Act 2010 Code of Practice. • Paragraphs 88 expanded re emphasis on preventative approach by Scottish Biometrics Commissioner. Paragraph 92 expanded re differentiation in regulatory landscape and guidance on complaints procedure to be published on Commissioner's website. Some proofing of references tidied in response to feedback from SPA Chair. • Principles 1,2,3,5,6,7,8,9,12 further expanded in response to feedback from ICO. Hyperlinks inserted to link readers to relevant ICO website guidance materials on UK GDPR and DPA 2018. • Minor points of clarification and proofing and typographical amendments highlighted by BFEG. • Appendix 'D' amended in response to feedback from BTP, MDP, and NCA to accommodate potential expansion to UK wide policing bodies operating in Scotland.
Version 0.4 Created March 2022	• Principle 10 updated to require data breaches reported to ICO to also be notified to Scottish Biometrics Commissioner. • Principle 12 updated to further clarify Age of Criminal Responsibility (Scotland) Act 2019 guidance following Scottish Government review.
Version 1.0 Created August 2022	• Approved by Cabinet Secretary for Justice and Veterans on 08 August 2022

Foreword

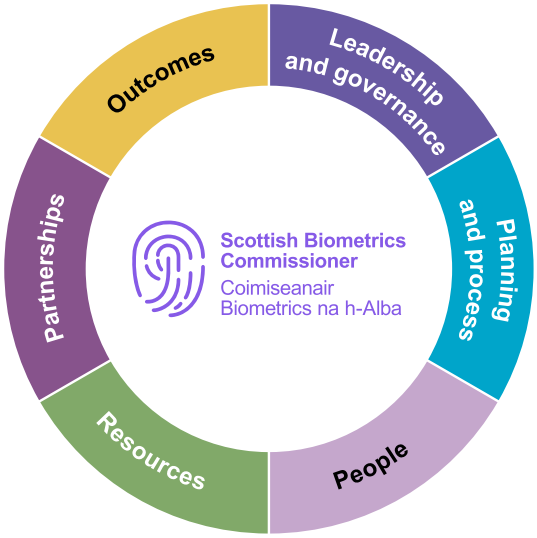
This Code of Practice has been prepared in accordance with the provisions of section 7 of the Scottish Biometrics Commissioner Act 2020 which provides that in furtherance of the Commissioner's general function, the Commissioner must prepare, and may from time-to-time revise, a Code of Practice on the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes in Scotland.

This Code seeks to promote good practice, transparency, and accountability in Scotland by setting out an agreed framework of standards for professional decision-making which strikes the right balance between the needs and responsibilities of policing and our criminal justice system in terms of enforcing the law and keeping citizens safe, and the fundamental obligation to guarantee the basic human rights, privacy, and freedoms of individual members of the public.

The Code of Practice has been developed following extensive and ongoing consultation and is structured around 12 Guiding Principles and Ethical Considerations to which Police Scotland, the SPA, and PIRC must adhere to when acquiring, retaining, using, or destroying biometric data for criminal justice and policing purposes in Scotland. These principles and ethical considerations form the basis against which compliance with this Code of Practice will be assessed.

The Guiding Principles and Ethical Considerations outlined in this Code of Practice are supported by a National Assessment Framework for Biometric Data Outcomes in Scotland.

The Assessment Framework has been developed by the Scottish Biometrics Commissioner in partnership with the Improvement Service and is based on the Public Sector Improvement Framework in Scotland.[1] The framework has 6 outcome headings and contains 42 individual quality indicators that have been nuanced to the biometric data context in Scotland.



These 6 outcome headings are:

- Leadership and governance
- Planning and process
- People
- Resources
- Partnerships
- Outcomes

This Code of Practice will be brought into effect by an instrument containing regulations laid before the Scottish Parliament and will be kept under ongoing review.

[1] Public Sector Improvement Framework (PSIF), Improvement Service: https://www.improvementservice.org.uk/products-and-services/performance-management-and-benchmarking/public-sector-improvement-framework

How to use this Code of Practice

This Code of Practice on the acquisition, retention, use, and destruction of biometric data for criminal justice and policing purposes in Scotland applies to Police Scotland, the Scottish Police Authority (SPA), and the Police Investigations and Review Commissioner (PIRC).

The Code of Practice is structured into 8 parts. Parts 1 to 4 of this Code contain introductory background information on biometric data and technologies in a policing and criminal justice context, including the existing legal framework in Scotland and the adopted definition of biometric data as set out by Parliament in the Scottish Biometrics Commissioner Act 2020.

The introductory materials also explain the legal exclusions to this Code of Practice. These may be summarised as biometric data acquired by UK wide policing bodies operating in Scotland under reserved powers and functions, where biometric data is acquired under legislation reserved to the UK Government, and when responsibility for regulatory oversight is already vested in another UK Commissioner.

Part 5 then contains the main substance of this Code of Practice. It details and describes the 12 Guiding Principles and Ethical Considerations to which Police Scotland, the SPA, and PIRC must adhere to ensure compliance with this Code of Practice.

Part 5 of this Code should also be read in conjunction with Appendix 'A' which contains an assessment framework of 42 quality indicators for biometric data outcomes. This tool is drawn from the quality assurance model and assessment framework adopted by the Scottish Biometrics Commissioner and is based on the Public Sector Improvement Framework (PSIF) in Scotland, which in turn is based on the European Foundation of Quality Management (EFQM) Business Excellence Model.[2]

The 12 General Principles and Ethical Considerations contain the information and substructure required to assess compliance with this Code of Practice. The Assessment Framework is intended to assist more generally in the evaluation of overall direction, execution, and results to help improve independent oversight, governance, and scrutiny. These sections also serve as a self-assessment checklist for the bodies to whom this Code of Practice applies in terms of supporting their own distinct internal governance arrangements.

Part 6 is forward looking. It outlines the considerations and recommended process for adopting future biometric technologies or new applications of existing technologies.

[2] The EFQM Model 2020: https://www.efqm.org/efqm-model

How to use this Code of Practice

Part 7 and 8 describe the arrangements set out in the Scottish Biometrics Commissioner Act 2020, for the Commissioner to monitor and report on the Code, including where necessary the service of compliance notices. These closing chapters also explain the legal mechanisms available to the Commissioner for addressing any failures to comply with this Code of Practice, albeit that the strategic emphasis from the Commissioner will be on encouraging and promoting compliance. Our legislation make provision for a procedure by which an individual, or someone acting on an individual's behalf, may make a complaint to the Commissioner. This procedure will be published separately.

As Scottish Biometrics Commissioner, I wish to record my thanks and appreciation to everyone who has contributed to the development of this Code of Practice. Their various contributions have helped to shape this Code and will greatly assist me in discharging my general function to support and promote the adoption of lawful effective and ethical practices in relation to the acquisition, retention, use, and destruction of biometric data for criminal justice and police purposes in Scotland.

Dr Brian Plastow
Scottish Biometrics Commissioner
November 2022

Summary of the 12 guiding principles & ethical considerations:

When acquiring, retaining, using, or destroying biometric data for criminal justice and policing purposes in Scotland, Police Scotland, the SPA and PIRC must adhere to the following 12 General Guiding Principles and Ethical Considerations.

A full description of each Principle, and the agreed framework of standards and ethical considerations can be found in Part 5 of this Code of Practice.

It should be noted that this Code of Practice applies to biometric data used for criminal justice and policing purposes only. It does not apply to biometric data given voluntarily by police officers and police staff and used for internal employment purposes.[3] Similarly, it does not apply to circumstances where members of the public request the police to take their fingerprints in support of applications for foreign Visas or other emigration purposes. See paragraph 21 of the Code for further information on areas to which this Code of Practice does not apply.

The 12 principles and ethical considerations:

1. Lawful authority and legal basis
2. Necessity
3. Proportionality
4. Enhance public safety and public good
5. Ethical behaviour
6. Respect for the human rights of individuals and groups
7. Justice and accountability
8. Encourage scientific and technological advancement
9. Protection of children, young people, and vulnerable adults
10. Promoting privacy enhancing technology
11. Promote equality
12. Retention periods authorised by law

[3] These matters are catered for in Police Scotland and SPA employment policies and procedures and in relevant professional standards guidance.

Contents


3

01
Background and purpose of the Code of Practice

Introduction to Code of Practice

1 Biometric data such as fingerprints and photographs have been used in policing and criminal justice in Scotland as a means of verification, identification, and exclusion for more than 100 years. Since the late 1980s, the advent of the forensic technique of DNA profiling has revolutionised the investigation of crime. It is used daily in the investigation of a wide range of offences to identify offenders from minuscule amounts of body fluids and tissues. In sexual offences, DNA profiling can untangle complex mixtures of body fluids, typically found in such cases, to provide evidence that was previously unavailable. Through the introduction of DNA24, Scottish Police Authority Forensic Services now provides Police Scotland and the Police Investigations Review Commissioner (PIRC) with one of the most advanced DNA interpretation capabilities in world policing.

2 More recently there has been an exponential growth in a range of new biometrics in law enforcement, perhaps most controversially the use of public space facial recognition surveillance by the police in other UK jurisdictions.[4] There has also been a proliferation of databases operating and exchanging biometric data over different legal and functional jurisdictions within the UK and globally, including the application of artificial intelligence (AI) to those databases to develop algorithms for biometric matching.

3 Such issues raise important questions for society, including how best to balance our need for public safety and security, with broader privacy, ethical, human rights, and equality considerations. The principles of proportionality and necessity, and the long-established principle of policing by consent in Scotland, suggests the need to be careful about the extent of future encroachment.

Scottish Biometrics Commissioner Act 2020

4 This Act was passed by the Scottish Parliament on 10 March 2020 and received Royal Assent on 20 April 2020. The Act established the office of Scottish Biometrics Commissioner and provides for its functions.

5 The Commissioner is independent of Scottish Government and is appointed by Her Majesty the Queen on the nomination of the Scottish Parliament. The Commissioner's general function is to support and promote the adoption of lawful, effective, and ethical practices in relation to the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes by Police Scotland, the Scottish Police Authority (SPA), and the Police Investigations and Review Commissioner (PIRC).

[4] R (Bridges) v CC South Wales [2020] EWCA Civ 1058.

6 In exercising that general function, the Commissioner is to:

- keep under review the law, policy and practice relating to the acquisition, retention, use and destruction of biometric data by Police Scotland, the SPA and PIRC.
- promote public awareness and understanding of the powers and duties those persons have in relation to the acquisition, retention, use and destruction of biometric data, how those powers and duties are exercised, and how the exercise of those powers and duties can be monitored or challenged.
- Promote, and monitor the impact of, the Code of Practice.

7 The Commissioner must also have regard to the technology used or capable of being used for the purpose of acquiring, retaining, using, or destroying biometric data.

8 Section 2 (6) of the Act requires that in the exercise of the general function, the Commissioner must have regard to the interests of:

- children and young persons, (defined as individuals under the age of 18 years) and,
- vulnerable persons (defined as individuals who, by reason of their personal circumstances or characteristics, may have difficulty understanding matters relating to the acquisition, retention, use and destruction of their biometric data).

Purpose of this Code of Practice

9 It is a fundamental value of our society that we respect the right of every person to go about their lawful business without unjustified interference from the State. Where the State does interact with any person, that interaction should be governed by a respect by the State for that person, and for that person's freedoms and rights. In all its interactions the State must act with fairness and integrity, and in compliance with the law. Policing and the work of our criminal justice system is an example of the interaction between the State and the individual, sometimes when the individual is at their most vulnerable. This Code must therefore be read considering these fundamental values.

10 Police work in Scotland is carried out in accordance with the notion of policing by consent and in accordance with the fundamental policing principles, agreed by Parliament and exemplified in the Police and Fire Reform (Scotland) Act 2012. These are:

- that the main purpose of policing is to improve the safety and well-being of persons, localities, and communities; and
- that the police should be accessible, engage with communities, and promote measures to prevent crime, harm, and disorder.

These principles inform all policing work in Scotland and, by extension, this Code of Practice.

11 Section 7 of the Scottish Biometrics Commissioner Act 2020 provides that in furtherance of the Commissioner's general function, the Commissioner must prepare, and may from time-to-time revise, a Code of Practice on the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes.

12 Accordingly, this Code seeks to promote good practice, transparency, and accountability in Scotland by setting out an agreed framework of standards which strikes the right balance between the needs and responsibilities of policing and our criminal justice system in terms of enforcing the law and keeping citizens safe, and the fundamental obligation to guarantee the basic human rights, privacy, and freedoms of individual members of the public.

13 Therefore, this Code of Practice has regard to the importance of:

a. promoting and protecting equality and human rights,

b. promoting and protecting an individual's right to privacy,

c. promoting and protecting public confidence in the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes,

d. ensuring the safety of individuals and communities,

e. balancing the public interest considerations with the rights of individuals, and

f. considering the serious human rights and ethical considerations of biometric data sharing and AI in technical processing.

Whom the Code applies to

14 Section 9 of the Biometrics Commissioner Act 2020 requires that the following must comply with the Code of Practice when exercising functions to which the code relates:

a. constables and police staff of the Police Service of Scotland,[5]

b. the Scottish Police Authority,

c. the Police Investigations and Review Commissioner.

Relevant enactments to which the Code will apply

15 The Scottish Biometrics Commissioner Act 2020 requires that the Code of Practice must include provision about when biometric data must be destroyed in cases where a relevant enactment does not make such provision and may make different provisions for different purposes. The relevant enactments specified in the Act are:

- Part 2 of the Criminal Procedure (Scotland) Act 1995,
- Section 56 of the Criminal Justice (Scotland) Act 2003,
- Chapter 4 of Part 4 of the Age of Criminal Responsibility (Scotland) Act 2019.

16 The Criminal Procedure (Scotland) Act 1995 is the primary criminal procedure legislation in Scotland which enables persons who have been arrested to have their fingerprints and DNA taken and for corresponding custody image and Criminal History System (CHS) photographs to be captured.[6]

[5] The terms 'constable' and 'police staff' have the same meanings as in section 99 (1) of the Police and Fire Reform (Scotland) Act 2012.

[6] Photographs are not explicitly referenced in the Criminal Procedure (Scotland) Act 1995, but it has been custom and practice for arrested persons in Scotland to be photographed for more than 100 years. The retention policy applied to criminal history photographs by Police Scotland is the same as that applied to fingerprints and DNA.

17 Section 56 of the Criminal Justice (Scotland) Act 2003, allowed for the establishment of a database of DNA profiles developed from persons who have supplied their written consent to have their DNA profiles retained for specific purposes, namely the investigation and prosecution of a single offence or more general retention which allows the volunteer's DNA profile to be examined for any other offences which may be investigated in future.
Section 56 also provides for the withdrawal of consent.

18 Chapter 4 of Part 4 of the Age of Criminal Responsibility (Scotland) Act 2019 details the limitations on taking prints and samples from children under 12 years of age and limitations on taking prints and samples from children aged 12 and over in certain circumstances.

19 In addition to legislation explicitly referenced in the Scottish Biometrics Commissioner Act 2020, this Code of Practice will also apply to other legislation which permits the capture of biometric data in Scotland by Police Scotland, the SPA or PIRC without consent, except where that data is collected under legislation reserved to the UK Parliament, and where it already falls within the independent oversight of another UK Commissioner. See paragraph 24 of this Code of Practice for information on excluded functions within the remit of other UK Commissioners.

20 One legislative framework not explicitly referenced in the Scottish Biometrics Commissioner Act 2020 is the Sexual Offender Notification Requirements (SORN) of Part 2 of the Sexual Offences Act 2003 in relation to Registered Sex Offenders (RSO). Section 87(4) of the Sexual Offences Act 2003 provides that when completing the SORN, the offender must, if requested to do so, allow the police to take fingerprints and to photograph any part of the offender's body. All RSO's must be photographed a minimum of every 12 months or sooner if their appearance changes.
The Police, Public Order and Criminal Justice (Scotland) Act 2006 also authorises the police and relevant staff to take relevant physical data (DNA) from an RSO as part of their SORN. Accordingly, such biometric data will fall within the oversight of the Scottish Biometrics Commissioner and the arrangements described in this Code of Practice.

21 In addition to computerised biometric data records arising from specific technical processing, the meaning of "biometric data" within the Scottish Biometrics Commissioner Act 2020, and consequentially this Code of Practice includes the source materials from which a corresponding biometric record can be derived. Examples of such materials include blood, saliva, hair etc. Such materials may be obtained from a known individual under specific legislative provisions in Scotland for the purposes of verification, identification, or elimination using statutory or Common Law powers. The substantive point to note is that this code covers both the computerised data itself, and the corresponding physical samples from which such data may be derived. This Code also applies to volunteer samples when given for policing or criminal justice purposes. However, this Code of Practice does not apply to biometric data provided to Police Scotland voluntarily by persons for non-policing and non-criminal justice purposes such as in support of applications for overseas employment and education visas, or fingerprints taken for overseas emigration purposes. Similarly, this Code of Practice does not cover biometric data used by police bodies where the data has been given voluntarily by employees for general employment purposes, for example photographs for warrant cards or where police officers fingerprint data is held in the 'Police Eliminations Database', or where biological samples such as a hair sample is given for employee substance misuse screening purposes.

Exclusion of UK-wide policing bodies operating in Scotland

22 This Code of Practice applies solely to policing and criminal justice functions within the devolved competence of the Scottish Parliament and therefore to Police Scotland, the Scottish Police Authority (SPA) and the Police Investigations and Review Commissioner (PIRC). Accordingly, this Code does not apply to other UK-Wide policing bodies operating in Scotland, or to the biometric data they collect when arresting or investigating citizens in Scotland.

23 This Code of Practice therefore does not apply to the UK National Crime Agency (NCA), British Transport Police (BTP) or the Ministry of Defence Police (MDP). However, those policing bodies have indicated a willingness to be included under the oversight of the Scottish Biometrics Commissioner when conducting policing functions in Scotland if the necessary legislative authority can be established. Accordingly, Scottish Government has submitted a request to the UK Government for a section 104 order under the Scotland Act, 1998.[7] Should an order be agreed between the Scottish and UK governments and approved by the UK Parliament, this Code will be amended accordingly to include such UK policing bodies operating in Scotland, and such bodies will be invited to sit on the professional advisory group of the Scottish Biometrics Commissioner.[8]

Excluded functions within remit of other UK Commissioners

24 This Code of Practice similarly does not apply to policing functions carried out by Police Scotland, SPA or PIRC under policy areas reserved to the UK Government, where responsibility for regulatory oversight is already vested in another UK Commissioner. For example, this Code of Practice does not apply to:

a. Biometric data in relation to which the Home Office Biometrics and Surveillance Camera Commissioner (BSCC) for England and Wales has a function under section 20 of the Protection of Freedoms Act 2012 specifically national security determinations (NSDs) in Scotland made under section 18G of the Criminal Procedure (Scotland) Act 1995.[9]

b. Matters in relation to which the Investigatory Powers Commissioner (IPCO) has responsibility under the Investigatory Powers Act 2016, and the Regulation of Investigatory Powers (Scotland) Act 2000.[10] It should also be noted that the Scottish Ministers have previously published separate Codes of Practice covering Covert Human Intelligence Sources (CHIS), Covert Surveillance, and Equipment Interference under section 24 of the Regulation of Investigatory Powers (Scotland) Act 2000. Targeted equipment interference is the process by which an individual's electronic equipment may be covertly interfered with to obtain information or communication. Activity could include remote access to a computer or covertly downloading mobile phone contents including personal data.

---

[7] Section 104 of the Scotland Act 1998 allows for consequential modifications to be made to reserved law in consequence of an Act of the Scottish Parliament.

[8] Ongoing discussions between Scottish and UK Governments do not include the Civil Nuclear Constabulary.

[9] Section 20 of the Protection of Freedoms Act 2012 makes provision for the Home Office Biometrics and Surveillance Camera Commissioner (BSCC) to keep under review national security determinations, including those made in Scotland, under section 18G of the Criminal Procedure (Scotland) Act 1995. A national security determination is made if the Chief Constable determines that it is necessary for biometric data to be retained for the purposes of UK national security.

[10] Regulation of Investigatory Powers (Scotland) Act 2000: Codes of Practice. https://www.gov.scot/publications/regulation-of-investigatory-powers-scotland-act-2000-codes-of-practice/

c. The enforcement of data protection and privacy laws including the Data Protection Act, 2018, the UK General Data Protection Regulation (UK GDPR) and the upholding of information rights in accordance with the statutory functions of the UK Information Commissioner (IC0).[11]

This Code therefore sits alongside and intersects with the developing framework in the rest of the UK for policing and criminal justice. This includes UK data protection law, guidance from the Biometrics and Surveillance Camera Commissioner for England and Wales, guidance from the IPC0, and guidance and authorised professional practice relative to biometrics and forensics from the National Police Chief's Council (NPCC), and Forensic Science Regulator for England and Wales.

Consultation on draft Code

25 Section 10 (1) of the Scottish Biometrics Commissioner Act 2020 requires that in preparing a draft Code of Practice, the Commissioner must consult:

a. the Scottish Ministers,

b. the Lord Advocate,

c. the Lord Justice General,

d. the Faculty of Advocates,

e. the Law Society of Scotland,

f. the Chief Constable of the Police Service of Scotland,

g. His Majesty's Inspectorate of Constabulary in Scotland,

h. the Scottish Police Authority,

i. the Police Investigations and Review Commissioner,

j. the Information Commissioner,

k. the Scottish Human Rights Commission,

l. the Commissioner for Children and Young People in Scotland, and

m. such other persons as the Commissioner considers appropriate.

[11] Responsibility for enforcing UK data protection law lies with the UK Information Commissioner (ICO). However, a finding by the ICO that Police Scotland, SPA or PIRC have breached data protection law in relation to biometric data could also constitute a breach of this Code of Practice.

26 Following initial consultation with the Commissioner's statutory advisory group established under section 33 of the Scottish Biometrics Commissioner Act 2020, the above bodies and office holders, and an extensive list of significant others, the Scottish Biometrics Commissioner prepared this updated draft for initial consideration by Scottish Ministers. Three impact assessment documents prepared by the Scottish Biometrics Commissioner accompany this Code and provide additional information on the consultation conducted.

27 In terms of section 11 of the Act, once the Commissioner has prepared a draft Code of Practice with which the Commissioner, with the consent of the Scottish Ministers, wishes to proceed, the Commissioner must lay a copy of it before the Scottish Parliament. In finalising a draft, the Commissioner must have regard to any representations about it that are made to the Commissioner within 60 days of the data on which the copy is laid before the Scottish Parliament.[12] In Spring 2022, the Commissioner lunched a public consultation on the Code of Practice.

Approval of the Code

28 Once the Commissioner has finalised a draft Code of Practice, the Commissioner must submit it to the Scottish Ministers for approval. The Scottish Ministers may approve a draft Code of Practice:

a. without modification, or

b. with such modifications as they, with the consent of the Commissioner, consider appropriate

If the Scottish Ministers do not approve a draft Code of Practice, they must give the Commissioner a statement of their reasons for not approving it.

Bringing the Code into effect

29 The Code of Practice once approved has no effect until the day appointed for the code by regulations made by the Scottish Ministers. Ministers must, when laying before the Scottish Parliament a draft of an instrument containing such regulations, also lay a copy of the approved Code of Practice. The Commissioner must publish the approved Code of Practice as soon as reasonably practicable after the regulations are made.

[12] In calculating the period of 60 days, no account is to be taken of any time during which the Parliament is dissolved or in recess for more than 4 days.

02
Meaning of biometric data in this Code of Practice

Legal definitions

30 The term 'biometric data' has not previously been defined in criminal justice legislation in Scotland.

31 Biometric data is however defined in the UK General Data Protection Regulations 2018 (UK GDPR). The UK GDPR forms part of the data protection regime in the UK, together with the Data Protection Act 2018 (DPA). Biometric data and genetic data are each classified as 'sensitive processing' under UK GDPR and can only be processed without the consent of the data subject where there is a clear lawful basis, such as law enforcement.

32 The UK GDPR defines biometric data in Article 4 (14) as '…personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'. The term 'dactyloscopic data' means fingerprint data. All biometric data is personal data within the UK data protection regime, as it allows or confirms the identification of an individual.[13]

33 However, for the purposes of this Code of Practice the adopted meaning of 'biometric data' is derived from Section 34 (1) of the Scottish Biometrics Commissioner Act 2020 which defines the meaning in the following terms:

> *"Biometric data"* means 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.
>
> For the purposes of subsection (1), *"biometric data"* may include:
>
> a. Physical data comprising or derived from a print or impression of or taken from an individual's body,
>
> b. A photograph or other recording of an individual's body or any part of an individual's body,
>
> c. Samples of or taken from any part of an individual's body from which information can be derived, and
>
> d. Information derived from such samples.

34 Accordingly, this Code of Practice applies to all computerised biometric data records, to any such data developed by Artificial Intelligence (AI) generated and/or machine learning technique, to corresponding manual prints, impressions, or photographs, and to biological samples or materials used for criminal justice and police purposes from which identity information about an individual can be derived. Subject of course to the specific exclusions previously stated in paragraphs 21 to 24. It should be noted that such biological samples and materials are referenced as 'genetic data' within the Data Protection Act 2018.

[13] Guide to the General Data Protection Regulation (GDPR), Information Commissioners Office: 2018

03
Biometric databases, technologies, and samples

Biometric databases and technologies

35 There are many different databases and technologies utilised for criminal justice and policing purposes in Scotland which acquire, retain, use, or destroy biometric data. Some of these databases and technologies are operated independently in Scotland whilst others are managed by the Home Office or National Police Chief's Council (NPCC) under joint UK funding arrangements and form part of a network of interrelated databases used for a range of UK national security and law enforcement purposes including policing and criminal justice.

36 For example, Scotland has its own DNA database (SDNAD) and sequencing and analysis technologies but also uploads records to the UK National DNA Database (NDNAD) maintained under joint funding arrangements by the Home Office. SPA Forensic Services provides Police Scotland and PIRC with one of the most advanced DNA profiling capabilities available in world policing. DNA profiling in Scotland looks at 24 areas of a person's DNA – a significant step up from the 11 areas that made up previous DNA profiling technology and an advance on the 17 areas used by most other UK police forces which is the NDNAD and European standard.

37 Similarly, Police Scotland operates its own Criminal History System (CHS) containing the criminal history records and photographic images of persons charged with, or convicted of, a common law crime or statutory offence in Scotland. These images on CHS are uploaded automatically to a UK policing intelligence sharing system known as the Police National Database (PND), so that other UK forces can search the PND to help identify and prosecute criminals. In the event of acquittal, the Scottish records and images are removed from CHS and PND by Police Scotland once notified of non-conviction or absolute discharge by the Crown Office and Procurator Fiscal Service (COPFS).[14] If a child is referred to the Children's Hearings system, images are destroyed.

38 Other databases containing photographs of persons captured as part of the criminal justice process in Scotland include custody systems data, related case management systems, intelligence databases, and potentially through other investigative techniques such as digital forensics where personal data such as a photographic image can be recovered from the personal device of a suspect or witness (for example a Smartphone) as evidential material during the course of an investigation, and where it may thereafter be stored electronically in a searchable format for investigative or evidential purposes.

[14] Such images are however retained if the subject already has a previous criminal conviction in Scotland.

39 Conversely Scotland does not have its own fingerprint database, but instead Scottish fingerprints whether initially captured optically or manually are uploaded to IDENT1 which is the UK central national database for holding, searching, and comparing data on those who encounter the police as detainees after being arrested. Information held includes fingerprints, palm prints and scenes of crime marks.

40 Except for the excluded and reserved functions as previously highlighted in this Code of Practice, it should be noted that the laws in Scotland governing the acquisition, retention, use and destruction of biometric data for criminal justice and policing purposes are different from other UK jurisdictions. Similarly, the operational policies, practices, and procedures of policing sector bodies in Scotland differ, as do the technical capabilities of many of the biometric technologies.

41 In addition, it should be noted that some other UK jurisdictions have authority in law to capture biometric data from citizens without their consent using mobile biometric technologies in circumstances where they have not been arrested. For example, the power under section 61 (6A) of the Police and Criminal Evidence Act 1984 which allows the police in England and Wales to fingerprint a suspect who has not been arrested and where they have refused to provide their name or are suspected of having provided false information. Such 'Identity Not Known' (INK) biometric technologies such as mobile fingerprint scanners have proved controversial and currently have no legal basis in Scotland.[15]

42 This contextual information is included in this Code of Practice to highlight how the operation of shared UK databases containing biometric data results in constitutional complexities and challenges when seeking to align divergent, devolved, and reserved policy imperatives around biometrics, as further complicated by the nuances of different legal policy frameworks in different UK legal jurisdictions that exist for both policing and criminal justice administration.

43 In 2016, and as a key finding in relation to the use of the Facial Search functionality within the UK Police National Database (PND) by Police Scotland, HM Chief Inspector of Constabulary in Scotland (HMICS) determined:

'…in contributing to UK policing systems, it is important that Police Scotland has the functionality to administer and maintain Scottish data in compliance with Scottish legislation and any Scottish Codes of Practice in terms of its use'.[16]

44 Accordingly, this Code of Practice will apply to all biometric data contained within databases and technologies utilised in Scotland by Police Scotland, the SPA and PIRC for criminal justice and policing purposes in Scotland, except in circumstances where independent oversight is already exercised by an existing UK Commissioner as explained earlier in this Code of Practice under reserved or excluded functions. This means that the Scottish Biometrics Commissioner will exercise independent oversight of all non-excluded biometric data held or used in Scotland, and over all non-excluded 'Scottish biometric data' including where it is held directly in shared UK technology systems such as IDENT1.

[15] Police use of fingerprint scanners disproportionately targets Black Britons, 3 November 2020: https://www.wired.co.uk/article/police-fingerprint-scan-uk

[16] [2016] HMICS, Audit Assurance of Facial Search Functionality within the UK Police National Database.

Forensic science samples

45 The national Forensic Science model in Scotland is also distinct. Forensic crime scene analysis in Scotland is provided to Police Scotland and PIRC by SPA Forensic Services to ensure differentiation or a sterile corridor to delineate the police or PIRC investigation from the scientific investigation. The national Forensic Science model in Scotland from crime scene to court is internationally acclaimed, and places quality and accreditation at the heart of everything. The sterile corridor principle, through differentiation, also exists to exonerate the innocent.

46 Most of the work of SPA Forensic Service has been accredited to deliver scientific and forensic services by the United Kingdom Accreditation Service (UKAS) for more than 20 years. Third-party assessment by UKAS accreditation offers confidence that forensic activities are carried out impartially and competently. Compliance with the relevant international ISO Standard infers the highest levels of personal conduct, and organisational compliance with quality management systems and standards.[17]

47 Scotland does not have a Forensic Science Regulator, but SPA Forensic Services adhere voluntarily to the Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System produced by the Home Office Forensic Science Regulator for England and Wales. These Codes of Practice cover incident scene examination, recovery of biological materials, obtaining DNA profiles and fingerprint comparison, and various other forensic disciplines.[18]

In the absence of a Forensic Science regulator for Scotland, this Code of Practice will also cover crime scene samples from which biometric data may be derived. Such samples are not covered in terms of section 18 A of the Criminal Procedure (Scotland) Act 1995, but it is important that they can be retained. This is important for unsolved crimes and in respect of cases which may be retried in terms of the Double Jeopardy (Scotland) Act 2011, as well as cases reported to the Procurator Fiscal where proceedings cannot be commenced at that time, but that may be dealt with should the doctrine of mutual corroboration come into play later.

Criminal justice and other samples

48 In addition to crime scene sampling and depending on the nature of the matter under investigation, biological samples (mouth swab for DNA, blood samples, hair samples etc.) can be taken from persons following arrest for identification, verification or elimination in the criminal justice process as previously described. This Code of Practice applies to the acquisition, retention, use and destruction of biometric data derived from such samples and to the corresponding acquisition, retention, use and destruction of the source sample materials. This includes criminal justice samples, evidential samples, elimination samples, and samples for other non-excluded policing purposes for example for inclusion in the Missing Person DNA Database.

[17] Where a body to whom this Code applies can demonstrate compliance with relevant ISO Standards and UKAS accreditation for DNA screening laboratory functions, fingerprint enhancement laboratory functions, and scenes of crime work, such quality assurance accreditation can be relied upon by the Scottish Biometrics Commissioner.

[18] Forensic Science Regulator, Codes of Practice and Conduct, For Forensic Science Providers and Practitioners in the Criminal Justice System, Issue 6: 2021.

04
The law, human rights and data protection

The law in Scotland – biometrics in the criminal justice process

49 This Code of Practice is necessary to ensure that the legal framework surrounding the acquisition, retention, use, and destruction of biometric data as part of the Criminal Justice Process in Scotland is understood, and that the retention of biometric materials and data by Police Scotland, the SPA and PIRC is both necessary and proportionate, and in accordance with the law. This Code of Practice also seeks to establish a framework of standards against which to measure the quality of systems, practices, and procedures in an area where biometric data is collected from people as part of the criminal justice process and mainly without the usual safeguard of consent.

50 The Criminal Procedure (Scotland) Act 1995 ('the 1995 Act') is the primary Scottish legislation allowing the retention of fingerprints and other samples from a person arrested by the police. Sections 18 to 19C stipulate the conditions under which samples may be taken by the police, as well as rules for retention and specification of the purposes of use of samples. It should also be noted that Section 18G permits biometric data to be retained for reserved matters, notably under national security determinations. The existing law may be summarised as follows:

- Fingerprint and DNA data from convicted persons can be retained indefinitely. This legal entitlement applies because of a single criminal conviction for any type of offence, regardless of the gravity of that offence.[19]
- Data from children dealt with at the Children's Hearing system may be retained only where the grounds of referral are established (whether through acceptance by the child at such a hearing or a finding in court) in relation to a prescribed sexual or violent offence. Such data can only be retained for three years unless the police apply for, and are granted, an extension by a Sheriff. For less serious offences, and where grounds are not established, there is no retention in relation to children.

[19] In Gaughran v. UK (February 2020) the European Court of Human Rights ruled that indefinite retention of biometric data without review was a breach of a person's right to respect for their private life under Article 8 ECHR. The Scottish Biometrics Commissioner's Strategic Plan 2021-2025 includes provisions for a review of the laws of retention for biometric data in Scotland.

- Data from individuals who accept certain Fiscal Offers may be retained for three years in relation to a prescribed sexual or violent offence, with the Chief Constable able to apply to the Sheriff Court for further two year extensions (there is no limit on the number of two year extensions that can be granted in respect of a particular person's data); and data may be retained for two years in relation to non-sexual or non-violent offences which are the subject of a Fiscal offer or fixed penalty notice from the police;

- Data from individuals prosecuted for certain sexual and violent offences may be retained for three years (whether or not they are convicted), with the Chief Constable[20] able to apply to the Sheriff Court for further two-year extensions (there is no limit on the number of two-year extensions that can be granted in respect of a person's data); and

- Subject to the exception just stated, data from individuals arrested for any offences (and who have no previous convictions) must be destroyed as soon as possible if they are not convicted or if they are given an absolute discharge.

51 Section 83 of the Police, Public Order and Criminal Justice (Scotland) Act 2006 inserted Section 18A into the 1995 Act and contains provisions to allow retention of DNA samples and profiles of persons where criminal proceedings were instituted. The list of relevant sexual and violent offences is in section 19A (6) of the Act, and Section 48 of the Crime and Punishment (Scotland) Act 1997.

52 In 2010, the Scottish Government also introduced sections 77 to 82 of the Criminal Justice and Licensing (Scotland) Act 2010 which included provisions to develop the law in relation to the retention and use of DNA, fingerprints, and other physical data. This was done by amendment to the 1995 Act.

53 In addition to primary Scottish legislation, the Sexual Offences Act 2003 provides the law to support the registration of sex offenders, and the restrictions and obligations placed on them, including the provision for the capture of biometric data as part of offender management processes. The 2003 Act is supplemented by the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005.

54 The Scottish Government will conduct ongoing reviews of the primary criminal justice legislation, and the Scottish Biometrics Commissioner will offer advice on biometric data. This includes a scheduled collaborative review of the laws of retention in Scotland as detailed in the Scottish Biometrics Commissioner's 4-year Strategic Plan laid before the Scottish Parliament on 24 November 2021. However, the foregoing sets out guidance in Scotland for the current legal framework for the acquisition, retention, use and destruction of biometric data by Police Scotland, the SPA and PIRC.

[20]These powers are currently preserved for the Chief Constable of the Police Service of Scotland (Police Scotland) and do not extend directly to the Chief Constables of BTP, MDP or the Director General of the NCA.

The law - Public sector equality duty (PSED)

55 To ensure compliance with this Code of Practice, Police Scotland, the SPA and PIRC should ensure that all standard operating procedures, policies, and practices relevant to the acquisition, retention, use and destruction of biometric data have undergone an equality and human rights impact assessment (EQHRIA) to ensure that such policies and practices do not discriminate unlawfully.

56 Under the Equality Act 2010, section 149 (Public Sector Equality Duty), public sector bodies must, in carrying out their functions, have due regard to the need to eliminate unlawful discrimination, harassment, victimisation and any other conduct which is prohibited by that Act, to advance equality of opportunity between people who share a relevant protected characteristic and people who do not share it, and to foster good relations between those persons. The Equality Act also makes it unlawful for police officers to discriminate against, harass or victimise any person on the grounds of the protected characteristics of age, disability, gender reassignment, race, religion or belief, sex and sexual orientation, marriage and civil partnership, pregnancy and maternity when using their powers.

57 In addition, the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012 places a responsibility on listed authorities to assess and review all policies and practices to ensure that it complies with the equality duty in the exercise of its functions. The Chief Constable of Police Scotland and the SPA Board are the relevant listed authorities and should ensure the way that biometric data is acquired, used, retained, and destroyed complies with their Equality Act duties.

The law - Human rights

58 The Human Rights Act, which incorporates the European Convention on Human Rights (ECHR) into UK law, sets out the fundamental rights and freedoms that everyone in the UK is entitled to, and makes it unlawful for a public authority to act in a way which is incompatible with Convention rights. Consequently, any policy and legal framework for its use must be consistent with the human rights framework, and other guarantees laid down by relevant data protection laws. The use of personal data is sensitive and must be protected from abuse and arbitrariness. The Human Rights Articles most relevant to this Code of Practice are Article 2 – the obligation of the State to protect the right to life, Article 8 – the right to respect for private life, home and correspondence, and Articles 9 to 11: protection of our democratic freedoms.

59 All biometric data constitutes personal data, therefore acquisition, use and retention is an interference with the right to private and family life and subject to conditions of Article 8. In relation to retention' the obvious approach is to have a presumption in favour of deletion following the expiry of any minimum retention period as prescribed in law. This Code of Practice therefore establishes a presumption of deletion for biometric data (in circumstances where the subject has no previous convictions) following the expiry of the relevant retention periods as prescribed or permitted in law. In deleting such data, Police Scotland, the SPA and PIRC must ensure that the biometric data records concerned are deleted not only from the primary database on which they are stored, but also from any secondary or tertiary databases onto which the data may have been replicated. In deleting such data, any corresponding physical samples must also be destroyed. Such destruction should take place as soon as reasonably practicable.

60 Human rights are a subject devolved to Scotland by the Scotland Act 1998. The Scottish Parliament has competence to observe and implement international human rights treaties. Public authorities such as Police Scotland, the Scottish Police Authority, and the Police Investigations and Review Commissioner must work within that legal framework which is binding.

The law - Data protection

61 Data Protection legislation in the UK provides a framework for the handling of personal data. In summary, personal data are data which relate to a living individual who can be identified from it directly or with other information, which is in the possession of, or is likely to come into the possession of, the data controller (i.e., the organisation using the information). This includes biometric data.

62 The Data Protection Act 2018 provides the legal framework for all processing of personal data throughout the UK. In May 2018, the new data protection regime took effect throughout the EU because of adoption by the EU of the General Data Protection Regulation (UK GDPR) and the Law Enforcement Directive (LED) as transposed into UK law. The DPA and UK GDPR should be read side by side as interlinking legislation and form the basis of UK data protection laws.

63 The revised UK data protection regime provides that general processing of personal data must be undertaken in compliance with the UK GDPR and processing for law enforcement purposes by designated or 'competent' authorities – i.e., named authorities with powers to investigate and/or prosecute crimes and impose sentences, together with certain other organisations must conform with the LED as transposed into UK law.

64 The UK GDPR extends the data protection regime in several ways. It updates the definition of personal data to reflect scientific and technological advances which have taken place since the passing of Directive 95/46/EC; it provides several enhanced rights for data subjects; and it requires data controllers to strengthen their governance procedures in relation to personal data.

65 The principles in Part 3, Chapter 2 of the Data Protection Act 2018 apply to biometric data processes for law enforcement purposes. For the purposes of this Part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

66 Both UK GDPR and the law enforcement provisions require that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. Additionally, the law enforcement provisions of the DPA require that logs be kept of any automated processing of personal data, i.e., where a system undertakes processing by automated means. The logs required include collection, alteration, consultation with, disclosure, combination, and erasure of personal data records.

67 Both the UK GDPR and the law enforcement provisions adopt a definition of personal data which explicitly includes biometric information within it as 'sensitive processing'. Any processing of biometric information must therefore be undertaken in compliance with either the UK GDPR or the DPA according to whether the processing is general processing or for law enforcement purposes. In this regard, biometric data are defined as personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images, fingerprints, or DNA.

68 Under Part 3 of the Data Protection Act 2018 'sensitive processing' can only be undertaken in two cases; where the individual has given consent (but note that there will be very limited circumstances where competent authorities can obtain valid consent for the processing) or where the competent authority can demonstrate that the processing is strictly necessary and satisfy one of the conditions in Schedule 8 of the DPA 2018. Strictly necessary means that the processing must relate to a pressing social need that cannot reasonably be achieved through less intrusive means. This is a requirement which will not be met if the purpose can be achieved by some other reasonable means.

69 To ensure compliance with this Code of Practice, Police Scotland, the SPA and PIRC must, in relation to the acquisition, retention, use and destruction of biometric data, comply with the provisions of the Data Protection Act (DPA), the UK General Data Protection Regulations (UK GDPR) and the Law Enforcement Provisions of the DPA 2018 (Part 3). This requires an 'appropriate policy document' to be in place, as described in either s35(4)b. or s35(5)c. as well as s42 DPA 2018. The policy document should contain:

- An explanation of how the processing complies with the relevant data protection principles; and
- An explanation of the controller's policies in relation to retention and erasure, including to give an indication of how long data is likely to be retained.

70 The competent authority's Data Protection Officer should give expert advice on data protection obligations that can inform the DPIA including the ICO consultation mechanisms in place under Part 3 of the DPA 2018. Links to the ICO guidance on DPIAs under Part 3 of DPA 2018 and to more detailed guidance on DPIAs under the UK GDPR are available on the ICO website.

05
General guiding principles and ethical considerations

Developing the right principles and ethical considerations

71 The following General Guiding Principles and Ethical Considerations provide summary information on considerations to be followed by Police Scotland, SPA and PIRC to ensure compliance with this Code of Practice on the acquisition, retention, use and destruction of biometric data for criminal justice and policing purposes in Scotland.

72 The content has been developed from a consolidated analysis of a range of sources including the enabling Scottish Biometrics Commissioner Act 2020, the relevant criminal procedure law in Scotland, other relevant legislation and guidance including the UK GDPR Criminal Offence data guidance, and the Data Protection Act 2018. It also embraces and hybridises the earlier seminal work of the Independent Advisory Group on Biometric Data in Scotland chaired by Lord Scott, Senator of the College of Justice in Scotland.[21] In a UK context, it embraces the 6 Governing Principles for biometric and forensic data analysis established by the Home Office Biometrics and Forensics Ethics Group (BFEG).[22] In international terms, it also draws on a contemporary literature review of international best practice guidance, including the 7 Ethical Principles for Biometrics produced by the Biometrics Institute in 2019.[23]

The 12 general guiding principles and ethical considerations

73 When acquiring, retaining, using, or destroying biometric data for criminal justice and policing purposes, Police Scotland, the SPA and PIRC should adhere to the following 12 General Guiding Principles and Ethical Considerations:

The following 12 Guiding Principles and Ethical Considerations form the core compliance features of this Code of Practice and should be read in conjunction with the associated 42 Quality Indicators in Appendix 'A'.

[21] Independent Advisory Group on the Use of Biometric Data in Scotland, Scottish Government: 2018.

[22] Biometric & Forensics Ethics Group (BFEG), Ethical Principles, December 2020.

[23] The mission of the Biometrics Institute is to promote the responsible and ethical use of biometrics and biometric analytics in an independent and impartial international forum for biometric users and other interested parties. The 7 Ethical Principles for Biometrics were published in 2019 and were compiled by a diverse group of international members and experts.

1 Lawful authority and legal basis

If you have official authority, you can acquire, retain, use, and destroy biometric data for criminal justice or policing purposes in Scotland without the consent of the data subject for those specific lawful purposes because you are processing that data in an official capacity. If you do not have such authority, you can only process criminal offence data without consent if you can identify a specific condition for processing in Schedule 1 of the Data Protection Act 2018. The basis of your lawful authority to acquire, retain, use, and destroy such data must be recorded in your relevant criminal justice or policing policies and procedures. The basis of your lawful authority should also meet the tests of necessity and proportionality and should avoid significant collateral intrusion.

Such lawful authority must be based in law and the law must provide a sufficiently clear and foreseeable basis for the processing. Specifically, it must have sufficient clarity and foreseeability to meet the standards required by the case law of the Court of Justice of the European Union and the European Court of Human Rights, as contemplated in Recital 33 to the EU Law Enforcement Directive.

Once biometric data has been collected for a specified, explicit, and legitimate purpose it should not be further processed in a manner that is incompatible with those purposes. Where a general, specific, or obligation to share data exists, then the legal basis for data sharing should be explicit in policy, process, and procedure.

Although it may be possible for competent authorities to gain valid consent in a few limited circumstances, these will be the exception rather than the rule. If biometric data is obtained from a crime victim or witness with their agreement and solely for elimination purposes, then such data should only be retained in connection with the case to which they relate.

Once the relevant case files are destroyed, the biometric records should also be destroyed. If such a crime victim or witness requests that their data is destroyed sooner, then the records should be destroyed in accordance with the wishes of the data subject (Section 56, Criminal Justice (Scotland) Act 2003).

If you acquire, retain, or use biometric data for criminal justice or policing purposes under other voluntary arrangements there should be a presumption of erasure or restriction and you should only retain such data with the express written consent of the data subject. Such a data subject (or someone acting in an official capacity on their behalf) may withdraw such consent at any time. This should be done verbally or in writing to the body holding the relevant data. The ICO guidance sets a statutory timeframe of one calendar month within which rights requests must be responded to.

Where consent to the holding of such data under voluntary arrangements is withdrawn, then that data can no longer be retained and should be destroyed as soon as reasonably practicable, providing that such removal will not, at the time of the request, conflict with any evidential requirement concerning the sample, data or information derived from it. Written confirmation should then be given to the data subject confirming that such data has been destroyed. The bar for valid consent under data protection and human rights is very high and is not met in circumstances where it cannot be freely withdrawn. Consent should be free, prior and informed.

Case files should be regularly reviewed and weeded in line with procedures that comply with the Fifth Data Protection Principle (Section 40, DPA 2018).

2 Necessity

If you have authority in law to acquire, retain, use, and destroy biometric data for criminal justice and policing purposes in Scotland, you should only do so if the processing operations, the category of data processed, and the duration of data kept is authorised in law, and is strictly necessary for those specific lawful purposes.

ICO guidance defines 'strictly necessary' as 'that the processing has to relate to a pressing social need, that cannot reasonably be achieved through less intrusive means.' As noted in Principle 1 above, the processing may be based on consent, but it is unlikely that there will be many circumstances in which the conditions for valid consent can be met.

3 Proportionality

If you have authority in law to acquire, retain, use, and destroy biometric data for criminal justice and policing purposes in Scotland, you should only take the necessary action needed for that specific lawful purpose and no more.

Proportionality under data protection law requires that the benefits of the activity outweigh the adverse impact of such processing on the rights of the data subject. It is for the controller to articulate how the processing of biometric data is proportionate in meeting the specified law enforcement purpose and in turn the demonstrable benefit to the public. How biometric processing, instead of possible other viable alternative means is proportionate to the criminal justice or policing purpose pursued and the supporting rationale should be documented in relevant policies and procedures.

4 Enhance public safety and public good

The way in which you acquire, retain, use, and destroy biometric data for criminal justice and policing purposes in Scotland should be informed by documented and published impact assessment processes. This is necessary to ensure that the processing of such data is in accordance with your statutory functions and enhances public safety and the public good or advances the interests of Justice and net benefits to society.

Relevant policies and procedures informing the acquisition, retention, use, and destruction of biometric data should have been subject to a Data Protection Impact Assessment (DPIA), a Community Impact Assessment (CIA), and an Equality and Human Rights Impact Assessment (EQHRIA). Biometric capture technologies and related databases should also be used in a way that enhances public safety and public good and should undergo similar DPIA, CIA and EQHRIA assessments. Such impact assessments should be published to demonstrate the importance of transparency in underpinning justice and accountability.

5 Ethical behaviour

Ethical behaviour means avoiding actions which may harm or disrespect people. The way in which you acquire, retain, use, and destroy biometric data for criminal justice and policing purposes in Scotland should be ethical and meet the requirements of law. This means that a culture of equality, fairness and social responsibility and wider community wellbeing should be promoted and encouraged amongst staff handling or processing biometric data.

Proposed new and revised policies and practices, and their supporting technologies should be impact assessed in line with the Public Sector Equality Duty (PSED) to eliminate discrimination and the Equality Act 2010 non-discrimination provisions.

When acquiring biometric data from individuals without consent, you should have a process in place which provides information to such persons of the legal reason for capturing their biometric data, including an explanation of the purposes for which that data will be used, and the circumstances under which it will be retained. The information should also include any complaint mechanisms available.

Staff working with biometric data and technologies should be familiar with the concept of unconscious or confirmation bias[24] and understand how the human interpretation of data can impact on equality, ethical, human rights and privacy considerations. Processes and procedures should be in place to acknowledge the limitations of biometric technologies and databases in terms of the potential for automated searches to produce both false positives and false negatives. Policies and procedures should acknowledge and seek to minimise errors resulting from the interactions between humans and technologies. Systems for staff working with biometric data and technologies should be quality assured to minimise error rates, and/or should be externally validated and accredited.

Biometric data acquired for a specific criminal justice or policing purpose in Scotland should not be shared for non-policing or non-criminal justice purposes in Scotland or with other jurisdictions except in accordance with the Data Protection Act 2018 and the Data Sharing Code of Practice produced by the UK Information Commissioner (ICO).
Data Sharing Code of Practice

Otherwise, data sharing between Scotland and other UK and International policing and criminal justice jurisdictions is encouraged within the context of existing treaties and safeguards. Within Europe this should be within the constraints of the UK Prüm arrangements for the exchange of fingerprints and DNA profiles between signatories to the Prüm Treaty for the purposes of law enforcement and national security.

[24] Confirmation Bias: A Ubiquitous Phenomenon in Many Guises, Nickerson R. S. Review of General Psychology 1998. Vol. 2, 175-220.

Otherwise, any other international exchanges should only take place within the context of important human rights safeguards and within the context of existing UK exchange mechanisms and treaties to safeguard against abuse. Preventing such abuses requires a 'human rights check' to take place in Scotland before any biometrics or other data are shared in the context of an international investigation. Serious human rights abuses – including assassination, kidnap, and torture of dissidents and/or their family members could occur if such safeguards are not followed.

Sharing with other UK and international policing bodies must be carried out in accordance with data protection law and policing bodies should formalise data sharing agreements for routine data sharing and devise plans that cover ad hoc or emergency data sharing. Data sharing taking place internationally needs to be in accordance with Part 3, Chapter 5 of the DPA 2018 and in accordance with ICO guidance on Law Enforcement processing and international transfers.

It is important to recognise that in many circumstances competent authorities will be unable to inform individuals when their biometric data is being processed because doing so would prejudice the law enforcement purpose. Nonetheless, relevant authorities should communicate openly and clearly with the public about how they intend to use and deploy biometric data and technology. This supports foreseeability and helps ensure that the processing is fair and within reasonable expectation. This can be done via privacy information, public consultation and engagement, and other communications tools.

Competent authorities should refer to the relevant ICO guidance including: the explaining decisions made with AI; the guidance on AI and data protection and toolkit for organisations considering using data analytics. Where Artificial Intelligence (AI) is being used it is of paramount importance that authorities demonstrate compliance with accountability, fairness and transparency and facilitate access to individual's information rights. In the majority of cases there is a legal requirement to complete a DPIA if you use AI systems that process personal data.

6 Respect for the human rights of individuals and groups

If you have authority in law to acquire, retain, use, and destroy biometric data for criminal justice and policing purposes in Scotland, you should do so with the utmost care and in a way which affords dignity and respect to the data subject and in a way that respects the rights to private and family life. You should also have respect for the human rights of individuals and groups and ensure that the way you deploy biometric technologies, or interpret biometric data, is non-discriminatory and does not unfairly target protected characteristic groups, religious groups, children, or other vulnerable individuals to whom protection from discrimination is afforded in law.

This Code of Practice also applies to biometric data relating to deceased persons given the extensive volume of data held. Clear protocols should be in place out of respect and dignity for the deceased. This principle goes beyond UK data protection law which only applies to the living.

Because biometric data retention is an interference with the right to privacy, this Code of Practice also establishes a presumption in favour of deletion and right of erasure following the expiry of any minimum retention period as prescribed in law in circumstances where the subject has no previous convictions. If a biometric data type has no retention period prescribed in law (for example photographs) then you should apply the same retention purpose and period of retention as you would for other types of biometric data, such as DNA and fingerprints in the corresponding case in question.

In deleting such data, you should ensure that the biometric data records concerned are deleted not only from the primary database on which they are stored, but also from any secondary or tertiary databases onto which the data may have been replicated. In deleting such data, any corresponding physical samples should also be destroyed. Such destruction should take place as soon as reasonably practicable having regard to the potential complications of linked cases, multiple offending, appeals by the prosecution, and the provisions of the Double Jeopardy (Scotland) Act 2011. Where data is retained beyond any period prescribed in law, explanatory case notes should be attached detailing why the data has not yet been destroyed.

7 Justice and accountability

This Code of Practice advocates the principles of openness, independent oversight, accountability, and the right of appeal and appropriate redress. Accessible, affordable, timely and effective remedies are a critical safeguard and complaint mechanisms play an important role in protecting against potential abuses and arbitrariness.

If you have authority in law to acquire, retain, use, and destroy biometric data for criminal justice and policing purposes in Scotland, you should have a complaints mechanism and appeals process in place which allows a data subject the right to redress where a data subject (or their designated representative) wishes to appeal against the holding of their biometric data. This may be encompassed within any generic complaints or quality of service concern mechanisms that you currently operate.

In addition, where an individual, or someone acting on an individual's behalf is of the opinion that a person required by section 9 (1) of the Scottish Biometrics Commissioner Act 2020, has specifically failed to comply with this Code of Practice, they may also make a complaint to the Commissioner. Such a complaint must relate solely to questions of compliance with this Code of Practice within the statutory complaints function of the Scottish Biometrics Commissioner.

Complaints about matters within the jurisdiction of the UK Information Commissioner (ICO) must be referred to the ICO. Any finding of a substantive breach of the Data Protection Act 2018 by the ICO may then be considered by the Scottish Biometrics Commissioner as a potential breach of this Code of Practice. These processes will be separate and the individual raising the complaint would need to raise a separate complaint with the Scottish Biometrics Commissioner following the ICO's adjudication.

The Commissioner will publish this procedure separately from this Code of Practice to demonstrate the importance of transparency in underpinning justice and accountability.

8 Encourage scientific and technological advancement

Systems for staff working with biometric data and technologies should encourage scientific and technological advancement and should be quality assured, and/or externally validated or accredited. Accredited techniques in forensic science should be adequately resourced to enhance forensic and biometric data capability and integrity, and to unlock value in accordance with the established crime scene to court model in Scotland.

The way in which you acquire, retain, use, and destroy biometric data for criminal justice and policing purposes in Scotland should encourage scientific and technological advancement to be harnessed to promote the swift exoneration of the innocent, afford protection and resolution for victims, and assist the criminal justice process.

However, you should also ensure that the use of any current or emerging biometric technologies in Scotland has a clear basis in law and that its use or intended use is both proportionate and strictly necessary. You should also ensure that the technology and the way that it is used or deployed is scientifically valid and reliable, that any algorithms for biometric matching are free from bias and are non-discriminatory on the grounds of race, gender, or any protected characteristic.[25] You should also ensure that the technology or the way that it is used or deployed does not result in significant collateral intrusion or impact negatively on public confidence, community cohesion, equality, human rights, or privacy considerations.

Where technology is provided by private industry (rather than the Home Office) the data controller (Police Scotland, SPA or PIRC) must ensure that the technology is fit for purpose before it is deployed and that it otherwise complies with the provisions of this Code of Practice. This will ensure that the entire end to end processing of biometric data for policing and criminal justice purposes is covered and that private contractors engaged by a body to whom this Code applies can be held to the same high standards by the contracting body. In such circumstances, the governance arrangements of the contracting body should:

- Build-in sufficient oversight of the processing carried out by third parties, including Data Protection Impact Assessments (DPIAs) being in place; and
- Ensure there is due diligence around transparency and effective limitation safeguards are in place.

Forward planning and early consideration of such technologies can facilitate compliance with and help controllers to mitigate any compliance issues before they arise. This could further ensure that data protection is integrated in the processing activities from the beginning. The completion and continual evaluation of DPIAs will be essential to this process.

[25] In the case of gender reassignment, it should be noted that a DNA profile will always determine the biological sex of the subject (birth sex) which may be different from the current legal sex.

It is likely that third parties, whether as a supplier or a processor, will be involved in the supply of new technologies and controllers will need to ensure that the supplier can provide the controller with sufficient detail about the proposed technology, particularly around storage, access, deletion, security, and risks so the controller understand the technology and can document this appropriately.

The ICO Accountability Framework, which has a section on Training and awareness, which in turn has a section on Specialised Roles highlights that those staff will require additional training and development and is a useful resource for data processors.

Appendix 'C' To this Code of Practice contains a process map outlining the considerations for introducing a new biometric technology or a new application to an existing biometric technology.

9 Protection of children, young people and vulnerable adults

If you have authority in law to acquire, retain, use, and destroy biometric data for criminal justice and policing purposes in Scotland, you should have policies and procedures in place to ensure the protection of children, young people, and vulnerable adults. This should additionally include the reasonable adjustments duty in relation to disabled people.

If relevant to your statutory functions, this should include the arrangements described in Chapter 4 of Part 4 of the Age of Criminal Responsibility (Scotland) Act 2019 including the limitations on taking prints and samples from children under 12, and the limitations on taking prints and samples from children aged 12 and over. Such policies should also cater for photographs and images of children.

You should also have policies and procedures in place to safeguard the interests of vulnerable persons. This means individuals who, by reason of their personal circumstances or characteristics, may have difficulty understanding matters relating to the acquisition, retention, use and destruction of their biometric data.

Individuals, under data protection law also have the right to be informed about the collection and use of their personal data and this Code advocates a requirement for outward facing documentation in relation to the acquisition, retention, use and destruction of biometric data that is particularly tailored to certain audiences such as children, young people and adults with additional support needs.

This may require consideration of the language used, the inclusion of infographics, videos, icons, or a layered approach. The information a controller must supply about the processing of personal data must be:

- concise, intelligible, and easily accessible;
- written in clear and plain language, adapting this to the needs of vulnerable persons, such as children; and
- free of charge

The right to this information is however a qualified right and subject to restrictions that prevent any prejudice to an ongoing investigation or compromise to operational techniques. The reliance on a restriction should be justified and applied as necessary and proportionate, and on a case-by-case basis. It is important that controllers balance the rights of the individual against the harm disclosure would cause.

10 Promoting privacy enhancing technology

The way in which you acquire, retain, use, and destroy biometric data for criminal justice and policing purposes in Scotland must ensure that such data is protected from unauthorised access and unauthorised disclosure in accordance with UK GDPR and the Data Protection Act 2018. You must also promote the highest quality of privacy enhancing technology use, including accuracy, error detection and repair, robust systems, and quality control. Such matters fall solely within the statutory remit of the Information Commissioner, however compliance with data protection legislation and UK Information Commissioner's Office (ICO) requirements in respect of biometric data is also a key compliance feature of this Code of Practice.

In addition to promoting privacy enhancing technology, the way that such technology is used must respect human rights, particularly Article 8 ECHR (respect for private life, family life, home, and correspondence).

The UK GDPR introduces a duty on all organisations to report certain personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible.

In addition to notification to the ICO, this Code of Practice mandates that if such a data breach or loss involving biometric data by an organisation to whom this Code applies occurs, then you must when notifying the ICO, also notify the Scottish Biometrics Commissioner. You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

11 Promote equality

The way in which you acquire, retain, use, and destroy biometric data for criminal justice and policing purposes in Scotland, or operate biometric technologies should comply with Section 149 of the Equality Act 2010 which requires all public authorities to:

- Eliminate discrimination, harassment, victimisation, and any other conduct that is prohibited by or under the Equalities Act 2010.
- Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

If you are a listed authority in terms of the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012 you also have a legal responsibility to assess and review all policies and practices to ensure that you comply with the equality duty in the exercise of your functions.

The Public Sector Equality Duty (PSED) applies to proposed new or revised policies and practices. Equality Impact Assessments should be kept under review and should be informed by appropriate monitoring. Reference should be made to the Equality Act 2010 Code of Practice: https://www.equalityhumanrights.com/sites/default/files/servicescode_0.pdf

In terms of this Code of Practice, you should have processes and procedures in place to ensure that the way that you acquire, use, retain, and destroy biometric data, and the way that you operate biometric technologies complies with the Equality Act 2010, and if applicable, the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012.

12 Retention authorised by law

Section 39, Part 3 of the DPA 2018 states that "Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes." Placing a responsibility on controllers to carry out periodic reviews of retained biometric data will ensure that the data held: is processed fairly (the first principle); is adequate, relevant and not excessive (the third principle); is accurate and kept up-to-date (the fourth principle); is not kept for longer than is necessary for the purpose for which it is processed (the fifth principle); and is securely kept, using appropriate technical and organisational measures (the sixth principle).

If you have authority in law to acquire, retain, use, and destroy biometric data for criminal justice and policing purposes in Scotland, then you must not exceed to the following permissible retention periods as prescribed in law.

ADULTS:

The existing law in Scotland provides that Fingerprint and DNA data from convicted persons can be retained indefinitely. This legal entitlement applies because of a single criminal conviction for any type of offence, regardless of the gravity of that offence. However, a review of the laws of retention in Scotland is now required and your data retention policy should instead reflect the European Court of Human Rights ruling in Gaughran-v-United Kingdom regarding the need to consider the proportionality of interference with Article 8 rights where there is indefinite retention of biometric material without periodic review.[26] In this judgment, the European Court of Human Rights found that: "the indiscriminate nature of the powers of retention of DNA profiles, fingerprints and photographs of the applicant as a person convicted of an offence, even if spent, without reference to the seriousness of the offence or the need for indefinite retention, and in the absence of any real possibility of review, failed to strike a fair balance between the competing public and private interests".

Photographic data from convicted persons does not currently have a prescribed period of retention in Scottish law. However, this Code of Practice advocates that where a specific legal purpose is applied to Fingerprints and DNA, then the same purpose and retention period should be applied to the photographic data applicable to that corresponding episode. Therefore, photographic data from convicted persons can be retained subject to the considerations mentioned regarding the Gaughran vs United Kingdom ruling.

Data from individuals who accept certain Fiscal Offers may be retained for three years in relation to a prescribed sexual or violent offence, with the Chief Constable able to apply to the Sheriff Court for further two year extensions (there is no limit on the number of two year extensions that can be granted in respect of a particular person's data); and data may be retained for two years in relation to non-sexual or non-violent offences which are the subject of a Fiscal offer or fixed penalty notice from the police;

Data from individuals prosecuted for certain sexual and violent offences may be retained for three years (whether or not they are convicted), with the Chief Constable able to apply to the Sheriff Court for further two-year extensions (there is no limit on the number of two-year extensions that can be granted in respect of a person's data); and

Subject to the exception just stated, data from individuals arrested for any offences (and who have no previous convictions) must be destroyed if they are not convicted or if they are given an absolute discharge. Although such destruction is specified in law as 'as soon as possible', operational practicalities necessitate that it should take place as soon as reasonably practicable, having regard to the need to manually weed physical samples and the potential complications of linked cases, multiple offending, appeals by the prosecution, and the provisions of the Double Jeopardy (Scotland) Act 2011. Where data is retained beyond any period prescribed in law, explanatory case notes should be attached detailing why the data has not yet been destroyed.

In all cases the retention of biometric data should be justified (with evidence to support the proposed retention periods) and only be kept for so long as is necessary for the purposes for which it is processed.

[26] Gaughran vs United Kingdom, Application No 45245/15, European Court of Human Rights, Strasbourg, 13 February 2020: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200817%22]}

CHILDREN:

The age of criminal responsibility in Scotland is twelve and the provisions of section 58(1) of the Age of Criminal Responsibility (Scotland) Act 2019 generally make it unlawful for the police to take prints or samples from a child under the age of twelve without an order from a sheriff (section 63). There is an exception to this prohibition where the child is an alleged victim of an offence, or of seriously violent, dangerous or sexually harmful behaviour by another child. Separate legislation allows for the taking of samples from child victims when they give their consent.

Where the situation is urgent and there is not time to obtain a court order in advance, non-intimate samples may be taken under section 69 with the authority of a senior police officer (not below the rank of superintendent). A court order to cover what has been done must be applied for subsequently.

Section 59(1) also generally makes it unlawful for the police to take prints or samples from a child aged twelve or over where this is to investigate an incident which occurred when the child was under twelve and they are suspected of having behaved in a seriously violent, dangerous or sexually harmful way. The police may take the prints or samples where authorised by a court order, using the power in section 69 (with a subsequent court application) or where the child consents.

It is important that investigators can exercise the normal powers open to them in relation to suspected child offenders twelve years of age or over in all other circumstances.

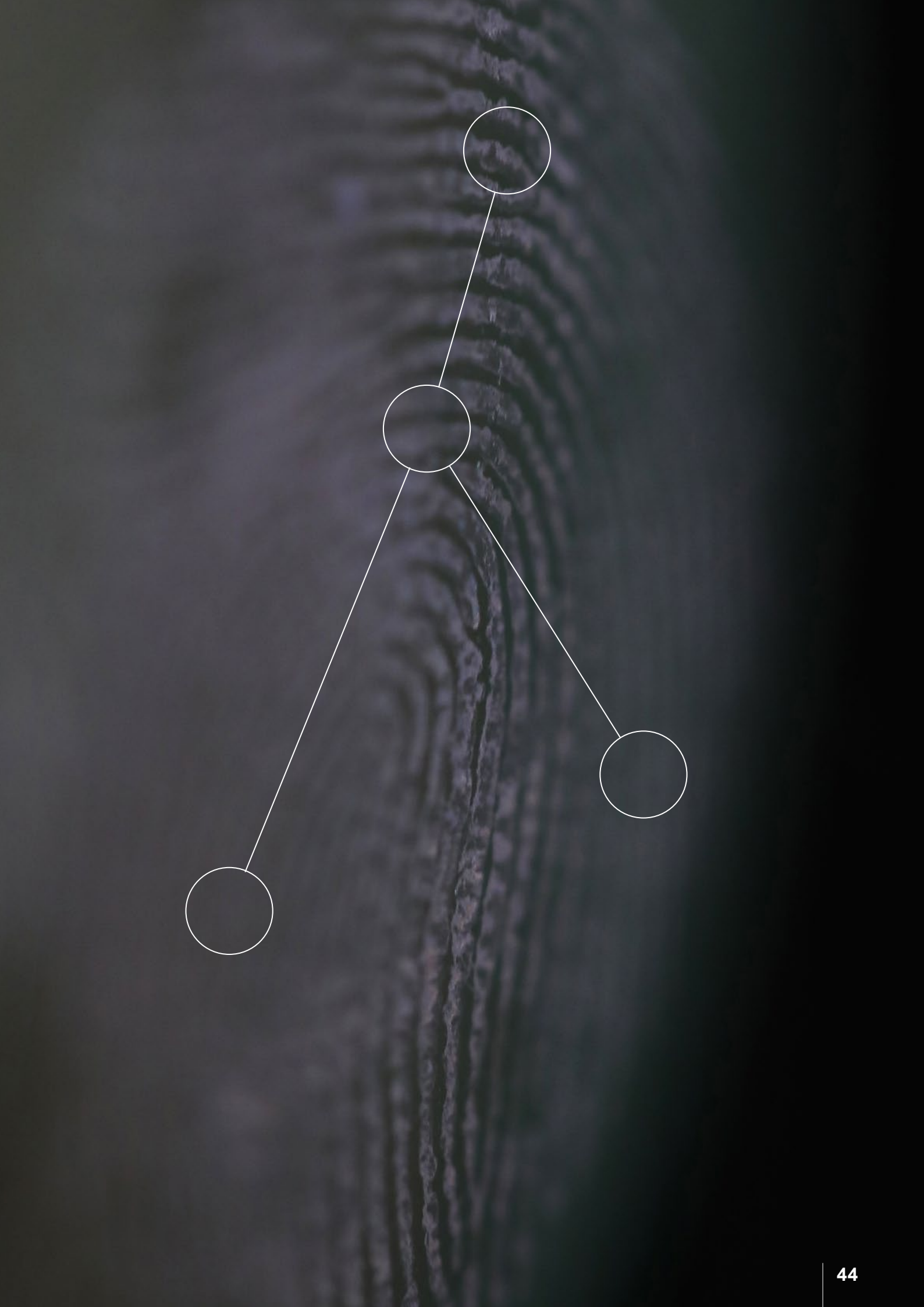
In Scotland, the legal status of a child is complex and defined differently by different pieces of legislation. The Children and Young People (Scotland) Act 2014 and the United Nations Convention on the Rights of the Child defines a child as someone under 18. However, the Children (Scotland) Act 1995, section 93, Criminal Procedure (Scotland) Act 1995, section 307, and Children's Hearing (Scotland) Act, section 199, all define a child as a person under 16 years of age; or a person aged 16 or 17 who is subject to a compulsory supervision order (CSO).

Section 2, of the Scottish Biometrics Commissioner Act 2020, provides for the functions of the Commissioner and section 2 (8) defines children and young persons as individuals under 18 years of age. In terms of this Code of Practice:

- Data from children dealt with at the Children's Hearing system may be retained only where the grounds of referral are established (whether through acceptance by the child at such a hearing or a finding in court) in relation to a prescribed sexual or violent offence. Such data can only be retained for three years unless the police apply for, and are granted, an extension by a Sheriff. For less serious offences, and where grounds are not established, there must be no retention in relation to children.

- The data from young people aged 16 or 17, not subject to a CSO, dealt with in the adult system will have the same corresponding periods of retention as specified for above for adults.

The processing of children's biometric data merits particular protection and particular care should be taken to ensure that it is fair. There should be a strong justification for any lengthy retention of children's biometric data and the risks associated with the processing must be recognised, assessed, and managed.



06
Process for adopting new biometric technologies

74 This Code of Practice is intended to provide an agreed framework of standards for the current use of biometric data for criminal justice and policing purposes in Scotland. Looking to the future, it also seeks to promote scientific and technological advancement particularly where such advancement in biometric data technologies advance the swift exoneration of the innocent, affords protection and resolution for victims, and assists the overall effectiveness and efficiency of policing and the criminal justice process.

75 In that sense, the guiding principles as set out in this Code of Practice also seek to provide a heuristic mechanism through which judgements can be formulated when considering whether a new biometric technology should be adopted in future, or when considering introducing a new application to an existing biometric technology. Of course, the fact that a new biometric technology is available does not necessarily mean that it should be adopted in a criminal justice and policing context in Scotland, particularly where the tests of lawfulness, proportionality and necessity cannot be met. Similarly, even if such a biometric technology passes the initial tests of lawfulness, proportionality, and necessity, it may still be unadvisable to proceed due to other factors such as the unavoidability of significant collateral intrusion, and/or where the intrusive nature or other factors might impact negatively on public confidence, community cohesion, the Public Sector Equality Duty, human rights, or privacy considerations.[27]

76 The main biometric data types used regularly in Scotland at present for policing and criminal justice purposes are Fingerprints, DNA and Photographic images. Fingerprints and DNA can be searched and compared automatically on policing databases to establish characteristics of 'uniqueness'. For example, the probability of two unrelated individuals having an identical DNA profile is around 1 in 1 billion. Although it should be noted that identical twins share identical DNA. Similarly, no two people (including identical twins) have ever been found to have identical fingerprints. By contrast, the facial search functionality within the UK Police National Database is based on an algorithm which looks for measurements of 'similarity' rather than uniqueness.[28] Against this context, it must also be understood that all such biometric technologies necessitate human interaction.[29] Accordingly mistakes can occur, and it is therefore important to acknowledge that there is no such thing as an entirely reliable biometric technology.[30]

[27] Privacy and Data Protection Issues of Biometric Applications, A Comparative Legal Analysis, Kindt E. J. Springer Law, Governance and Technology Series 12, London: 2013

[28] Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND), HMICS: 2016

[29] Our Biometric Future, Facial Recognition Technology and the Culture of Surveillance, Gates K. A., New York University Press, London: 2011

[30] When Biometrics Fail, Gender, Race and the Technology of Identity, Magnet S. A., Duke University Press, London: 2011

77 There are currently many other biometric modalities in use in other policing jurisdictions and in other public and commercial contexts, including many with potential applications to policing and criminal justice in the future. Examples of other modalities include vein pattern recognition, iris and retina recognition, gait recognition, ear recognition, hand and finger geometry recognition, voice recognition, and keystroke recognition to name but a few. Appendix 'B' to this Code of Practice gives explanatory context to each of these biometric modalities. It should be noted that this list of modalities is indicative rather than exclusive.

78 This leads naturally to questions of the most appropriate process through which to assess whether future technologies or new applications to existing technologies should be adopted. In a broader UK context, the Home Office Biometrics Strategy has established such a process, but that process is restricted to the content of a Data Protection Impact Assessment (DPIA) being validated or challenged at various stages of consideration, and additionally through the advice of an independent Privacy/Ethics Group.[31]

79 The need for an ethical process through which to inform decision making has been emphasised in recent years through police 'experimentation' with biometric technologies in other UK jurisdictions with software and hardware provided through private sector partnerships such as the use of facial recognition surveillance. Most notably, on 11 August 2020, the Court of Appeal of England and Wales found that an operational deployment of Automated Facial Recognition technology (AFR) by South Wales Police was 'unlawful' because of planning shortcomings which culminated in the potential violation of human rights and the breaching of privacy, data protection, and equality regulations.[32]

80 The process through which decisions about the adoption of new technologies in policing in Scotland are made has also been at the fore of political debate in recent years. For example, in April 2019, Members of the Scottish Parliament's Justice Sub-Committee on policing asked Police Scotland to cease their deployment of cyber-kiosks until there was greater clarity on the legal framework for their use.[33] This was subsequently established, and an agreed process of safeguards was introduced. In April 2020, these issues were further explored in the report of the multi-agency Digital Forensics Working Group (DFWG) report to the SPA Forensic Services Committee, which highlighted how both biometrics and digital forensics intersect at various points with almost identical privacy, human rights, community impact, and ethical considerations.[34]

[31] Home Office Biometrics Strategy 2018, page 16, Figure No 3: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf

[32] Bridges v South Wales Police, Case No: C1/2019/2670, 11 August 2020: https://www.judiciary.uk/wp-contentuploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

[33] MSPs call for rollout of police 'cyber kiosks' to be paused, 08 April 2019: https://www.parliament.scot/newsandmediacentre/111642.aspx

[34] A report to the SPA Forensic Services Committee: on options for the future delivery, accreditation, oversight and governance of digital forensics in Scotland, April 2020: https://www.spa.police.uk/media/flediwqv/rep-b-20200424-item-8-digital-forensics-wg-report.pdf

81 Against this context, Section 2 (4) of the Scottish Biometrics Commissioner Act requires the Commissioner to have regard to the technology used or capable of being used for the purpose of acquiring, retaining, using, or destroying biometric data thus providing a statutory responsibility to maintain oversight of new and emerging technologies. Similarly, Section 33 of the Act requires that the Commissioner must establish and maintain an advisory group, and that the purpose of that group is to give advice and information to the Commissioner about matters relating to the Commissioner's functions.

82 The Advisory Group membership is attached to this Code of Practice as Appendix 'C'. The Advisory Group provides a repository of relevant expertise well placed to consider, evaluate, validate, challenge, and advise the Commissioner on legal, ethical, equality, privacy, or community impact considerations arising from the potential adoption of new biometric technologies. Thus, the Advisory Group can also assist in informing the independent decisions of the bodies to whom this Code applies as to whether to proceed with a new biometric technology or new application to an existing technology, in accordance with the independent exercise of their respective statutory functions.

83 This Code of Practice therefore includes provision for the Scottish Biometric Commissioner and the Commissioner's Advisory Group to independently offer ethical advice to Police Scotland, the SPA, and PIRC on request when considering introducing a new biometric technology, or a new application to an existing biometric technology. This is catered for in the power to work with others outlined in section 3 of the Scottish Biometrics Commissioner Act 2020. The advocated interface with the Scottish Biometrics Commissioner and Advisory Group and the process for considering a new biometric technology is illustrated in a schematic attached as Appendix 'D' to this Code of Practice.

07
Monitoring and reporting on the Code of Practice

84 The Scottish Biometrics Commissioner must keep the approved Code of Practice under review, prepare and publish a report on the Commissioner's findings, and lay a copy of the report before the Scottish Parliament. The first report must be laid before the Parliament no later than 3 years after the date on which the first Code of Practice comes into effect. Subsequent reports must be laid before the Parliament no later than 4 years after the date on which the last such report was laid.

85 On 24 November 2021 the Scottish Biometrics Commissioner's 4-year Strategic Plan (2021 to 2025) was laid before the Scottish Parliament.[35] The Commissioner's Strategic Plan sets out how the Commissioner proposes to perform the Commissioner's functions during the period covered by the plan and sets out:

a. What the Commissioner's objectives and priorities are for that period,

b. How the Commissioner proposes to achieve them,

c. What the timetable is for doing so, and

d. What the estimated costs are of doing so

86 In addition to the 4-year Strategic Plan, the Commissioner has published a national Assessment Framework for Biometric Data Outcomes in Scotland.[36] This document sets out the quality management system to be used by the Commissioner to assist in discharging the Commissioner's functions and duties including the production and monitoring of the Code of Practice. The framework has 6 outcome headings and contains 42 individual quality indicators that have been nuanced to the biometric data context in Scotland. These 42 quality indicators are attached as Appendix 'A' to this Code of Practice and may also serve as a self-assessment framework for Police Scotland, the SPA, and PIRC in relation to the lawful, effective, and efficient management of biometric data and technologies.

[35] Scottish Biometrics Commissioner Strategic Plan 2021 to 2025: Strategic Plan 2021-2025 | Scottish Biometrics Commissioner

[36] Scottish Biometrics Commissioner National Assessment Framework, 2021: National Assessment Framework | Scottish Biometrics Commissioner

87 The Commissioner's 4-year Strategic Plan, Assessment Framework for Biometric Data Outcomes and the 12 Guiding Principles of this Code of Practice, (as agreed through consultation with Police Scotland, the SPA and PIRC) collectively provide the strategic framework within which compliance with this Code of Practice will be monitored and assessed by the Commissioner.

88 Importantly, the general powers conferred on the Scottish Biometrics Commissioner in section 4 (1) of the Act provide that:

'The Commissioner may do anything which appears to the Commissioner:

a. To be necessary or expedient for the purposes of, or in connection with, the performance of the Commissioner's functions, or

b. To be otherwise conducive to the performance of those functions'

89 Therefore, the Commissioner has wide ranging powers and authority in law to support and promote the adoption of lawful, effective, and ethical practices in relation to the acquisition, retention, use and destruction of biometric data in Scotland for criminal justice and policing purposes, and to do anything necessary in connection with the Commissioner's functions. In this regard, and when assessing compliance with this Code, the Commissioner will invest significant effort in a preventative approach to support improvement across the criminal justice landscape in line with recognised best practice prior to any enforcement activity.

08
Compliance with the Code

Complaints about failures to comply with the Code

90 Section 15 of the Scottish Biometrics Commissioner Act 202 requires that the Commissioner must provide a procedure by which an individual, or someone acting on an individual's behalf, may make a complaint to the Commissioner that a person who is required by section 9 (1) to comply with the Code of Practice has not done or is not doing so in relation to the individual's biometric data.

91 The complaints function of the Commissioner therefore provides a mechanism for complaints to be made by members of the public, or someone acting on their behalf, in circumstances where they consider that Police Scotland, the SPA, or PIRC have failed to comply with this Code of Practice in relation to the individual's biometric data. Therefore, any such complaints must firstly relate to matters within the scope of this Code of Practice, and secondly to the biometric data of that individual.

92 The Act also provides that the Commissioner's complaints procedure should be available regardless of whether the individual has already instigated a complaint through the complaints mechanism of the body they are complaining about.

93 The Scottish Biometrics Commissioner's complaints mechanism will be published separately from this Code of Practice. The complaints mechanism shall be accessible and inclusive, with both on and offline means of engaging. The Commissioner will also make reasonable adjustments to the complaint mechanism where appropriate. The complaint mechanism will provide additional information on the differentiation in the regulatory landscape and guidance on what regulator should be contacted in what circumstances. For example, highlighting the primacy of the Information Commissioner (ICO) on complaints relating to data protection matters.

Power to gather information

94 Section 16 of the Act affords the Scottish Biometrics Commissioner power to gather information from Police Scotland, the SPA, or PIRC via a written information notice specifying the requested information needed to investigate and establish whether there has been a failure to comply with this Code of Practice. Section 17 of the Act caters for any failure to comply with an information notice without reasonable excuse, and for any obstruction of the Commissioner's complaints investigation function to be reported by the Commissioner to the Court of Session.

Reports and recommendations

95 Section 20 of the Act provides that if the Commissioner determines that a person who is required by section 9 (1) to comply with the Code of Practice has not done so or is not doing so, the Commissioner must prepare and publish a report about that failure unless the Commissioner considers that it is sufficiently minor not to merit it. Such reports must be laid before the Scottish Parliament.

96 Section 21 of the Act provides that where such a report includes a recommendation to Police Scotland, the SPA, or PIRC then there is a requirement to respond. Section 22 of the Act provides that responses to such reports and recommendations must be published by the Commissioner and that a copy must be laid before the Scottish Parliament.

Compliance notices

97 Section 23 (1) of the Act provides that where the Commissioner considers that Police Scotland, the SPA, or PIRC has not complied or is not complying with this Code of Practice then the Commissioner may issue a compliance notice. A 'compliance notice' is a notice requiring the person to whom it is issued to take the steps set out in the notice to address the person's failure to comply with the Code of Practice. Further detail on compliance notices can be found in sections 23 to 26 of the Act.

Failure to comply with a compliance notice

98 Section 27 of the Act provides that where a person to whom a compliance notice has been issued refuses or fails, without reasonable excuse, to comply with the notice, the Commissioner may report the matter to the Court of Session.

99 After receiving such a report and hearing any evidence or representations on the matter, the Court may (either or both):

a. make such order for enforcement as it considers appropriate,

b. deal with the matter as if it were a contempt of court.

Further reading

100 Various sections of this Code of Practice summarise key aspects of the enabling legislation. For further detail and more comprehensive information on the various provisions of the Scottish Biometrics Commissioner Act 2020 can be accessed via the following link:

https://www.legislation.gov.uk/asp/2020/8/contents

Glossary

ACRA	Age of Criminal Responsibility Scotland Act 2019 (enacted 17/12/21)
AFR	Automated Facial Recognition
AI	Artificial Intelligence
BFEG	Biometrics and Forensics Ethics Group (Home Office)
BSCC	Biometrics and Surveillance Camera Commissioner
BTP	British Transport Police
CHIS Source	Covert Human Intelligence
CHS	Criminal History System
CNC	Civil Nuclear Constabulary
CIA	Community Impact Assessment
CNC	Civil Nuclear Constabulary
COPFS	Crown Office and Procurator Fiscal Service
DNA	Deoxyribonucleic acid
DFWG	SPA Digital Forensics Working Group
DPA	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
ECHR	European Convention on Human Rights
EQHRIA	Equalities and Human Rights Impact Assessment
HMICS	His Majesty's Inspectorate of Constabulary in Scotland
ICO	UK Information Commissioner
IPCO	UK Investigatory Powers Commissioner
IDENT1	UK National Fingerprint Database
LED	Law Enforcement Directive
MDP	Ministry of Defence Police
NCA	National Crime Agency
NDNAD	UK National DNA Database
PIRC	Police Investigations and Review Commissioner
PSED	Public Sector Equality Duty
PSIF	Public Sector Improvement Framework
RSO	Registered Sex Offender
SDNAD	Scottish DNA Database
SORN	Sex Offender Notification Requirements
SPA	Scottish Police Authority
UKAS	United Kingdom Accreditation Service
UK GDPR	UK General Data Protection Regulations 2018

Appendix A
Assessment framework
Quality indicators for biometric data

The tables below provide the details of the quality indicators that will be considered for each theme of the Scottish Biometrics Commissioner's assessment framework for biometric data. The framework of indicators is designed to help evaluate overall direction, execution, and results and to help improve independent oversight, governance, and scrutiny. These indicators are also intended for self-assessment with the aim of identifying strengths and areas for improvement that can be built into an Improvement Plan.

A. Outcomes (Results) - statements and self-assessment checklist	
A1	a. Strategies, Standard Operating Procedures (SOPs), and policies are in place for the acquisition, retention, use and destruction of biometric data and samples, and are regularly reviewed. b. The outcomes whether for verification, identification, or elimination purposes are clearly articulated in key policy documents and demonstrate a contribution to national priorities and outcomes.
A2	a. There are measures in place to monitor the outcomes from biometric data analysis and comparison. For example, data on Criminal Justice (CJ) Profiles added and removed, the matching of CJ Profiles to Crime Scene Profiles to assist crime solvency, data on crime scene match rates etc. b. Such data is published and updated on a regular basis to promote public understanding and awareness.
A3	a. The demand for the acquisition of biometric data through criminal justice sampling following arrest, and the demand from the creation of biometric samples derived from crime-scene materials are monitored and understood. b. The information is used to make improvements in the way services are prioritised, resourced and delivered.
A4	There are clear indicators of effectiveness and efficiency linked to strategic priorities and outcomes. For example, the utilisation of complex DNA analysis and interpretation to support or discount investigative hypotheses.
A5	Evidence and measures collected as part of a comprehensive performance management framework are compared with relevant benchmarks and trends, are appropriately segmented by biometric data category, (for example fingerprints, DNA, photographs) and are used to understand strengths and areas for improvement.
A6	Qualitative measures are in place to assess low volume but high value outcomes. For example, to adequately capture the value of advanced DNA profiling technology and tangible outcomes in terms of offering powerful new insights to current or cold case investigations.
A7	Performance management enables the demonstration of quality of service and best value, linking effectively with risk management and continuous improvement processes.

B. Leadership and governance - statements and self-assessment checklist	
B1	a. Criminal Justice and/or Forensic Science strategies for biometric data are clearly communicated. b. The principles of lawfulness, proportionality and necessity are embedded in the leadership and governance regimes in pursuit of national outcomes.
B2	a. Leaders promote a culture of effectiveness, efficiency and sustainability and drive and support change, improvement, and best value having considered relevant data and emerging trends. b. A culture of integrity, fairness, respect, and the protection of human rights is applied to leadership and governance considerations.
B3	Data security, community impact, equality impact, and privacy impact assessments are conducted in respect of biometric data and technologies ensuring that ethical and human rights considerations are embedded into operational practice and policy.
B4	a. Leaders actively build, support, and participate in strategic partnerships including UK leadership, governance, and oversight arrangements for biometric and forensic data. b. Governance arrangements are in place to ensure that Scottish law and policy is applied to the governance of Scottish biometric data collections when aggregated to UK biometric databases.
B5	There are clear governance and accountability arrangements for the organisation in relation to biometric data that hold leaders to account for delivering services effectively and efficiently
B6	There is effective, objective, and transparent scrutiny that allows challenge of strategy and policy implementation, decision making and performance.
B7	a. Performance and delivery against outcomes are reported to relevant staff, partners, the public and stakeholders. b. This is used to facilitate continuous improvement.

C. Planning and process - statements and self-assessment checklist

C1	a. There are organisational structures, strategies, policies, plans and processes in place for the management of biometric data. b. The acquisition, retention, use and destruction of biometric data is based in law and where legal gaps exist it otherwise adheres to the Code of Practice developed by the Scottish Biometrics Commissioner. c. Planning and processes support the delivery of desired outcomes effectively and efficiently.
C2	Key processes (including statutory duties) are mapped, reviewed, and improved. These consider the impact they may have on other areas of the organisation or other organisations, including processes undertaken in partnership.
C3	A culture of innovation, learning and improvement is promoted by identifying internal and external risk factors and good practice that could impact upon the delivery of outcomes and priorities. Information is shared widely to facilitate improvement.
C4	a. Changes to the way that biometric data or technologies is managed takes place through a structured process to ensure the defined impact and benefits from improvement actions are realised at an appropriate pace. b. The reliability of biometric technologies capable of automated search and comparison are validated and accredited.
C5	a. Engagement with the public, partners and stakeholders is an integral part of planning and improving services. b. Information on biometric data is available in ways that meet community needs and preferences. c. Safeguards and special arrangements are in place when collecting biometric data from children, young people, and vulnerable persons.
C6	There are effective complaints procedures, which include a commitment to investigate and resolve them within a defined time limit. This information is used to improve services.
C7	There are effective quality assurance and audit processes for biometric data sets and corresponding sample capture techniques to support learning and continuous improvement.

D. People - statements and self-assessment checklist

D1	There are appropriate structures and processes in place to support core values and ensure that staff working with biometric data and technologies have the skills and competencies required to deliver on agreed outcomes and priorities.
D2	a. A culture of equality and fairness, social responsibility and contribution to wider community wellbeing is promoted and encouraged. b. Staff working with biometric data and technologies are familiar with the concept of unconscious bias, and understand how the use of data can impact on equalities, ethical, human rights and privacy considerations
D3	Effective communication and engagement strategies are in place that meet the needs of staff and keep them informed and involved.
D4	People acquiring, retaining, using, or destroying biometric data understand the outcomes and priorities they are working towards, and their contributions are valued and recognised.
D5	People are encouraged to share information, knowledge and good practice and are involved in reviewing and improving the organisation while working together as a team.
D6	a. Systems for staff working with biometric data and technologies are quality assured, and/or are externally validated or accredited. b. People's performance is reviewed, and appropriate training and development opportunities provided, including induction processes and refresher training.
D7	The impact that the investment in training and development has had on the performance and service delivered is evaluated.

E. Resources - statements and self-assessment checklist

E1	Investment decisions in biometric data and technologies align to strategy and are subject to the production of robust business cases which are appropriately prioritised and scrutinised through internal and external governance. Business cases have clearly articulated benefits which can be measured as part of performance reporting.
E2	Organisations collecting biometric data for criminal justice and policing purposes in Scotland have the resources to manage and control Scottish biometric data in accordance with Scottish legislation, operational policies, and any Codes of Practice in terms of its use. This should include mechanisms to control the quality and use of that data when aggregated to shared UK databases such as IDENT1, NDNAD and PND.
E3	There is a clearly aligned financial strategy, financial management and governance processes for biometric databases and technologies which include risk assessment and transparent reporting.
E4	Information and intelligence are managed appropriately, and staff have access to the information they require to make evidence-based decisions and deliver effective, efficient, and improving services.
E5	Biometric data is effectively protected and made available securely to appropriate and relevant people and partners in accordance with privacy laws including UK GDPR, the Data Protection Act 2018, and guidance from the UK Information Commissioner (ICO) on the processing of biometric data for law enforcement purposes. Data sharing with other agencies complies with the ICO Code of Practice on Data Sharing.
E6	The benefits, opportunities, and risks of using digital technologies are understood. Technology is used effectively and efficiently to support operational strategy, manage resources and assets, and support and improve services.
E7	Accredited techniques in forensic science are adequately resourced to enhance forensic and biometric data capability and integrity, and to unlock value in accordance with the established crime scene to court model in Scotland.

F. Partnerships - statements and self-assessment checklist

F1	There is an agreed vision, purpose and objectives for partnership work involving biometric data or technologies that supports the delivery of national outcomes for Scotland.
F2	Strategic partnership arrangements for the exchange of biometric data for policing and criminal justice purposes within Scotland prioritise and manage shared opportunities and risks.
F3	Strategic partnership arrangements for the exchange of Scottish biometric data with other UK and international jurisdictions prioritise and manage shared opportunities and risks.
F4	The nature and extent of financial investment in shared UK biometric databases maintained for policing and criminal justice processes is understood and supports the delivery of policing priorities, justice priorities and/or national outcomes for Scotland.
F5	Effective governance arrangements are in place to manage, deliver, and review partnerships and progress against shared outcomes and priorities.
F6	Partnership exchange of biometric data supports effective service delivery and outcomes for communities. The impact and outcome of partnership activity is measured and understood.
F7	The exchange of Scottish biometrics data contained within UK policing databases such as IDENT1, NDNAD or PND with non-policing functions of the Home Office has a clear legal basis in Scotland, and agreed data control mechanisms determine the purpose, means, and safeguards, for the exchange and processing of sensitive personal data.

Appendix B
Summary overview of types of biometric data

DNA Matching
DNA matching facilitates the identification of an individual using analysis of the segments from their DNA. To compare a victim's or suspect's DNA profile to recovered crime scene DNA, the forensic science laboratory will compare the DNA within biological samples. DNA databases facilitate the automated recognition of samples. It should be noted that identical twins share identical DNA.

Fingerprint Recognition
Comparison of the unique ridges and valley patterns of a fingerprint or palm print to establish the unique identity of a person. Fingerprint databases and static and mobile optical scanners facilitate the automated recognition of samples.

Face Recognition
The comparison of 'similar' facial features or patterns to assist in the identification of an individual. Most live or real-time face recognition systems use either eigenfaces or local feature analysis. Eigenface is the name given to a set of vectors which produce measurements of the human face for automated analysis and identification by computers. Face recognition looks for similarity rather than uniqueness. It is a less reliable biometric.

Facial Search
The comparison of 'similar' facial features carried out retrospectively by comparing a single 'probe' image from a crime scene or incident against a gallery of images to assist in the potential identification of a suspect. This is the technology used within the UK Police National Database (PND). The objective is the for the software to produce a short-list of potential matching images that can then be further investigated by humans.

Other Images
It is common for other images to be held for policing and criminal justice purposes. Such images could include indecent images of children, victim injury images, suspect images from crime scenes or images taken on a police officer's personal digital assistant (PDA). This category does not however include routine images from drones or body worn cameras if such data is not used for evidential purposes or to profile an individual.

Eyes – Iris Recognition
The use of the features in a human iris to assist in the identification of an individual. Iris scanners collect around 240 biometric features, the amalgamation of which are unique to every eye. The scanners create a numeric representation of information extracted from the iris which is stored in a computer database to facilitate automated searching.

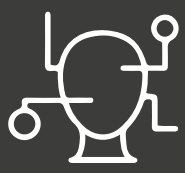
Eyes – Retina Recognition
The use of unique patterns of veins in the back of the eye to accomplish identification. The retina is the layer of blood vessels situated at the back of the eye. The scanners create a numeric representation of information extracted from the retina which is stored in a computer database to facilitate automated searching.

Ear Recognition
The identification of an individual using the unique shape of the human ear. An optical scanner produces an algorithm based on the curved features of an ear and is stored in a computer to facilitate automated searching.

Hand or Finger Geometry Recognition
The use of 3D geometry of the fingers and hand to facilitate the comparison of ‘similar’ facial features or patterns to assist in the identification of an individual.

Gait Recognition
The use of an individual’s walking style or gait to assist in automated recognition. Artificial intelligence systems are used to measure body mechanics for comparison with reference samples in a database.

Keystroke Recognition
Keystroke recognition or keyboard dynamics uses a unique biometric template to identify individuals based on typing pattern, rhythm, and speed. The raw measurements are known as ‘dwell time’ and ‘flight time’. Dwell time is the duration that a key is pressed, and flight time is the duration between keystrokes.



Vein Pattern Recognition
Vein pattern recognition technology is a method of biometric identification that looks for similarity or uniqueness on vein patterns of the human hand and forearm. The technique was first pioneered in Scotland by Professor Sue Black.

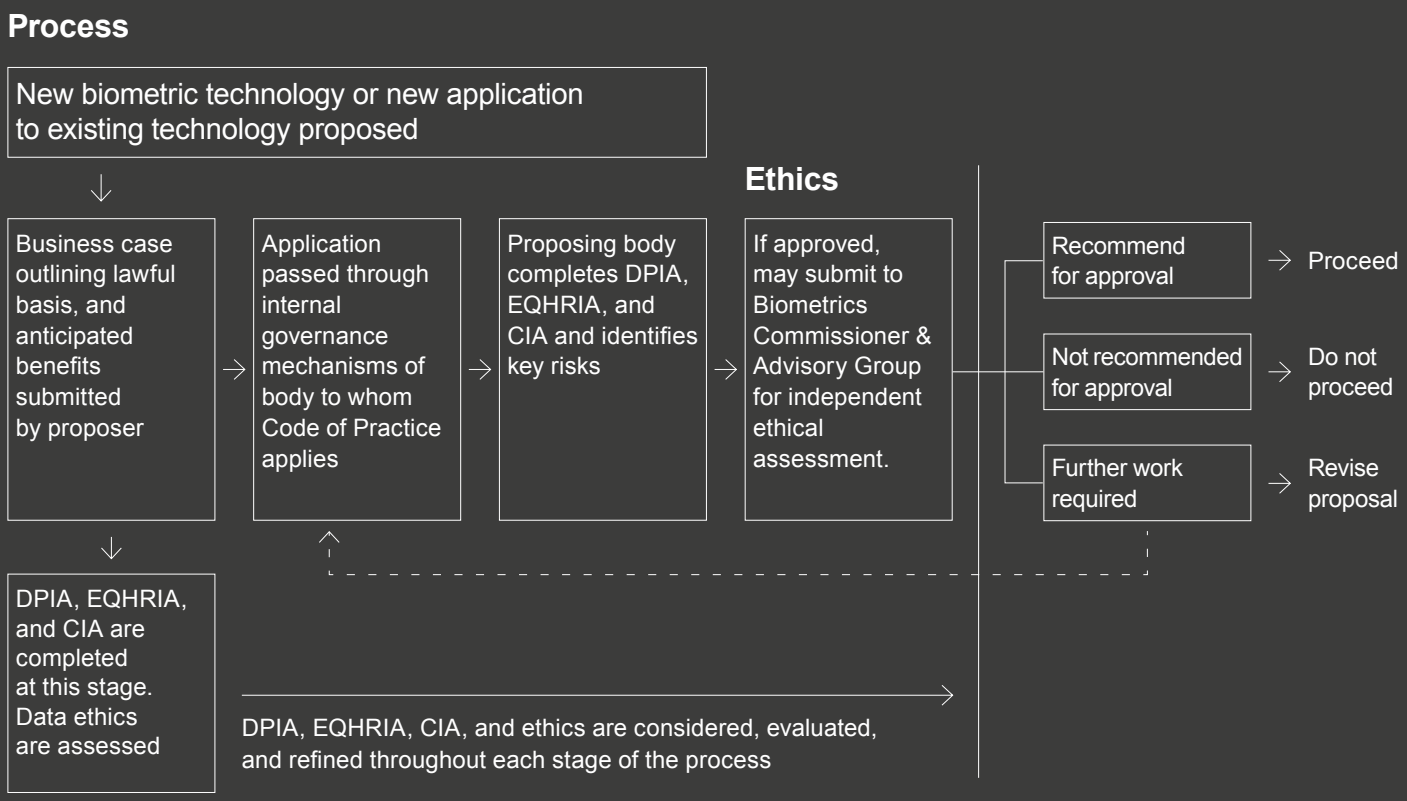
Voice Recognition
Voice biometrics is a technology which uses an algorithm to create a computerised voice print to assist with biometric identification. It is more commonly used for authentication rather than identification.


POLICE

Appendix C
Advisory group on biometric data and technologies - Membership

Director of Forensic Services	Scottish Police Authority Forensic Service
Professor John McNeill	Independent member and former PIRC Commissioner
HM Chief Inspector of Constabulary in Scotland	HMICS
Professor Shannon Vallor	Baillie Gifford chair in the Ethics of Data and Artificial Intelligence at the Edinburgh Futures Institute (EFI) at University of Edinburgh
Professor Derek Penman QPM (Independent Chair)	International Policing Consultant, former Chief Police Officer & Chief Inspector of Constabulary
Professor Fraser Sampson	Biometrics & Surveillance Camera Commissioner (E & W)
Detective Chief Superintendent	Police Scotland – Major Crime and Public Protection
Director of Investigations	Police Investigations & Review Commissioner (PIRC)
Procurator Fiscal	Crown Office and Procurator Fiscal Service (COPFS)
Head of ICO Regions	Information Commissioners Office (ICO)
Dr Genevieve Lennon	Chancellor's Fellow, University of Strathclyde
Chief Data Officer	Police Scotland
Head of Policy	Children & Young Persons Commissioner for Scotland
Head of Data Governance	Police Scotland
Operations Manager & Corporate Services Manager	Scottish Biometrics Commissioner
Biometrics Policy Lead	Scottish Human Rights Commission
Head of Change and Operational Scrutiny	Scottish Police Authority
Head of Policy	Mental Welfare Commission for Scotland.

Appendix D
Process for introducing a new biometric technology or a new application of an existing biometric technology for policing and criminal justice purposes in Scotland.



Scottish Biometrics Commissioner

Coimiseanair Biometrics na h-Alba

Safeguarding our biometric future