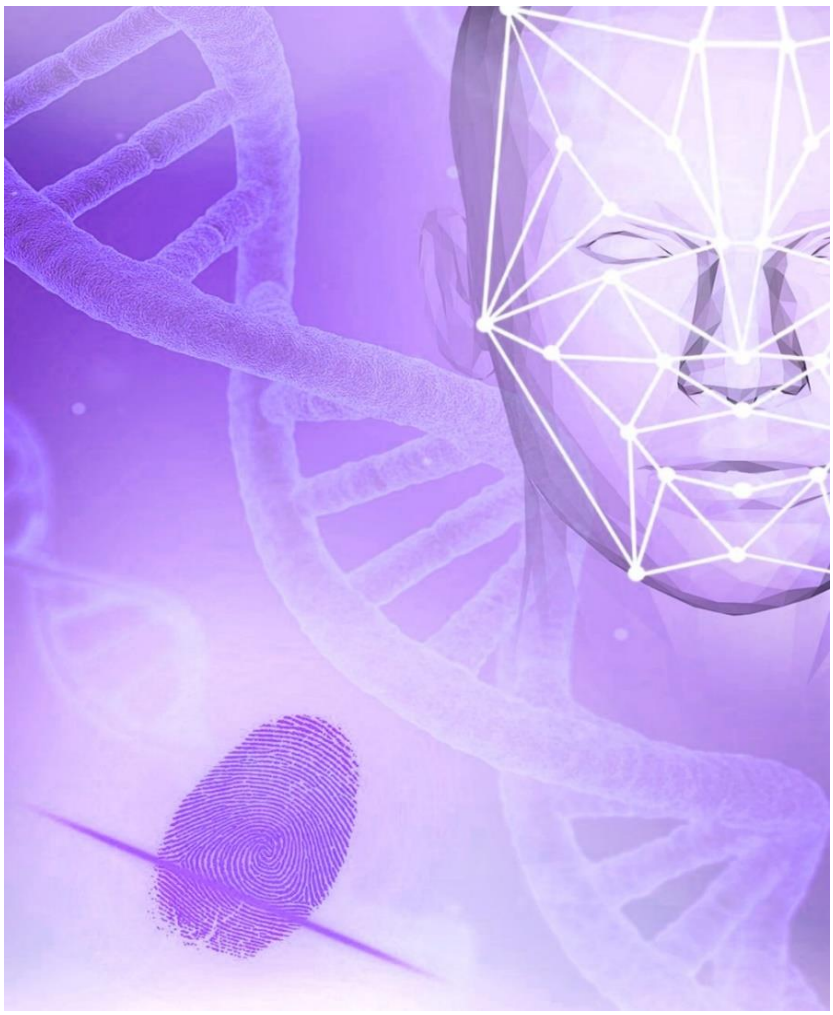
Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

SCOTTISH BIOMETRICS COMMISSIONER

RECORDS MANAGEMENT PLAN



Safeguarding our biometric future

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Document Control:

Title	Records Management Plan
Prepared by	Cheryl Glen
Reviewed by	Dr Brian Plastow
Version Number	2.0
Date	July 2023

Document amendments in this version	
V2	▪ Amendment to Element 8 reflecting Terms of Supply document ▪ Amendment to page 15 and reference to Data Protection Act 2018 ▪ Updates to numerous hyperlinks

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Contents

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Introduction

Under The Public Records (Scotland) Act 2011 (the Act) Scottish public authorities are required to produce and submit a Records Management Plan (RMP) setting out proper arrangements for the management of an authority's public records to the Keeper of the Records of Scotland (the Keeper) for their agreement under section 1 of the Act. The scope of the Records Management Plan applies to all records irrespective of the technology used to create and store them or the type of information they contain.

The Public Records (Scotland) Act 2011

Section 1 of the Act says,

(1) Every authority to which this Part applies must:

a) prepare a plan (a 'records management plan') setting out proper arrangements for the management of the authority's public records
b) submit the plan to the Keeper for agreement and
c) ensure that its public records are managed in accordance with the plan as agreed with the Keeper.

The Act specifically requires a public authority to include certain elements in its records management plan and it is unlikely the Keeper would agree a RMP that does not include these elements.

Records Management Plan

The Plan has 15 elements, which are:

1) Senior management responsibility
2) Records manager responsibility
3) Records management policy statement
4) Business classification
5) Retention schedules
6) Destruction arrangements
7) Archiving and transfer arrangements
8) Information security
9) Data protection
10) Business continuity and vital records
11) Audit trail
12) Competency framework for records management staff
13) Assessment and review
14) Shared information
15) Public records created or held by third parties

Element 1 – Senior management responsibility

An individual senior staff member is identified as holding corporate responsibility for records management.

Statement of Compliance

The Commissioner has overall strategic accountability for records management and accepts overall responsibility for the Records Management Plan that has been submitted. This is listed as one of the duties of the Commissioner's post and is evidenced by the job description.

Evidence of Compliance

- Commissioner's job description
- Records Management Policy within SBC Information Governance Handbook

Further Developments

There are no planned future developments.

Assessment and Review

Any staff changes will not invalidate this plan as all records management responsibilities will be transferred to the incoming post holder and relevant training will be undertaken.

Responsible Officer

The Commissioner – Dr Brian Plastow

Element 2 – Records manager responsibility

An individual staff member is identified as holding operational responsibility for records management and has appropriate corporate responsibility, access to resources and skills.

Statement of Compliance

The Corporate Services Manager has operational responsibility and ensuring organisational compliance for records management in SBC. The Corporate Services Manager is responsible for day-to-day records management; for the implementation of the SBC's Records Management Plan and the activities described in the elements. The Corporate Services Manager is the Keeper's initial point of contact for records.

Evidence of Compliance

- Corporate Services Manager job description
- Statement from Commissioner
- Records Management Policy within SBC Information Governance Handbook

Further Developments

There are no planned future developments.

Assessment and Review

Any staff changes will not invalidate this plan as all records management responsibilities will be transferred to the incoming post holder and relevant training will be undertaken. Training and development needs are monitored and reviewed annually to ensure post-holders with records management responsibilities have the necessary skills and experiences to carry out their tasks.

Responsible Officer

Corporate Services Manager – Cheryl Glen

Element 3 – Records management policy statement

The authority has an appropriate policy statement on records management.

Statement of Compliance

SBC recognises that the effective management of our records is essential in order to support our functions, to comply with legal, statutory and regulatory obligations and to demonstrate transparency and accountability to all of our stakeholders. Our commitment to effective records management is set out in our corporate Records Management Policy contained within our Information Governance Handbook. The policy and handbook are easily accessed by all SBC staff and both have been approved by the Commissioner.

SBC follows and complies with the best practice and guidance on the keeping, management and destruction of records set out in the Section 61 Code of Practice on Records Management by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002.

Evidence of Compliance

- Records Management Policy within SBC Information Governance Handbook

Further Developments

There are no planned future developments.

Assessment and Review

Our Records Management Policy is subject to ongoing monitoring and review to ensure that it continues to reflect the organisation's position towards record keeping.

Responsible Officer

Corporate Services Manager – Cheryl Glen

Element 4 – Business classification

Records are known and are identified within a structure, ideally founded on function.

Statement of Compliance

SBC manages its current records through a Business Classification Scheme (BCS) implemented within the Scottish Government's electronic records and documents management system, eRDM. This system is configured to the Scottish Government's business classification scheme, which has been adapted from the Integrated Public Sector Vocabulary Scheme (IPSV).

SBC records are mostly administrative in function or support our legislative function, they are easily defined, highly structured and whose access and retention are clearly determined. The SBC business classification system is modelled on the functions of the organisation and directly reflects the hierarchical relationship of functions, activities, transactions and records.

The Commissioner initially identified the organisation's core functions, component activities and associated transactions in order to develop the core structure of the file plan. The file plan is reviewed and adjusted in response to business needs when required. The file plan is actively used in the eRDM system's records centre, the central repository for all records managed in the system.

The SBC operates a paper-less office and does not keep any paper records. However, our financial processing and human resource management functions are provided to us under a shared services agreement with the Scottish Public Services Ombudsman (SPSO), and as approved by the Parliament Corporation, any paper records held for those purposes by the SPSO cannot be accessed by the Commissioner or SBC staff and form part of the arrangements described within the agreement.

Evidence of Compliance

- Business Classification Scheme (BCS) within SBC Information Governance Handbook
- Shared Services Agreement
- File Plan

Further Developments

Assessment and Review

The management of SBC records and the BCS are subject to ongoing monitoring and annual reviews to ensure that all of the functions, activities and transactions carried out by the SBC continue to be accurately represented within it.

Responsible Officer

Corporate Services Manager – Cheryl Glen

Element 5 – Retention schedules

Records are retained and disposed of in accordance with the Retention Schedule.

Statement of Compliance

The SBC Retention and Disposal Schedule identifies the record types created by the organisation and their recommended retention periods, in line with statutory and legislative obligations, as well as business need. The retention schedule is mapped to the topical structure of the Scottish Government Business Classification Scheme and reflects the retention and disposal actions used within the eRDM system. The retention schedule identifies records which are vital to operations and also records of enduring value which should be preserved in the archives. It serves as a reference point for all staff when assessing how long they need to retain business information and is actively used.

Emails stored on the Exchange Server are subject to the retention periods defined in the Scottish Government's Email Archiving Policy.

The SBC File Type Guidance - Retention and Disposal is published on our website. The guidance is based on the Scottish Government's guidance and describes the list of records for which pre-determined disposal dates have been established and the archiving and destruction arrangements that are in place.

Our Information Governance Handbook includes our Retention and Disposal Policy.

Evidence of Compliance

- File Type Guidance - Retention and Disposal
- Records Management Policy within SBC Information Governance Handbook

Further Developments

We are currently developing a stand-alone disposal policy in relation to complaints received against the Code of Practice to ensure all personal data is manually deleted after a 26 month period.

Assessment and Review

The retention schedules used within SBC are subject to ongoing monitoring and review to ensure they continue to identify all record types created in SBC and their appropriate retention periods.

Responsible Officer

Corporate Services Manager – Cheryl Glen

Element 6 – Destruction arrangements

Records are destroyed in a timely and appropriate manner and records of their destruction are maintained.

Statement of Compliance

The SBC File Type Guidance - Retention and Disposal is published on our website. The guidance is based on the Scottish Government's guidance and describes the list of records for which pre-determined disposal dates have been established and the archiving and destruction arrangements that are in place.

Destruction arrangements for electronic records contained in the filing system are managed in-house using the electronic file management arrangements contained within eRDM. Any manual disposal of electronic records according to the policy is managed by the Corporate Services Manager with assistance from the Business Support Officer. The SBC uses the SCOTS Connect service and staff use Microsoft 365 Apps for Enterprise for email management and Enterprise Vault for email archiving.

As we are a paperless office and do not keep paper records, there is no requirement to destroy paper records. However, in the instance where we do receive a paper record from a third party we scan and store as a pdf within eRDM and immediately destroy the original via the SPSO who have a contract with Paper Shredding Services (PSS) who dispose of paper securely. They comply with Code of Practice BS EN 15713:2009.

Evidence of Compliance

- File Type Guidance - Retention and Disposal Policy
- Corporate Services Manager job description
- Business Support Officer job description
- Records Management Policy within SBC Information Governance Handbook
- SPSO arrangements – Procedures and Paper Shredding Services

Further Developments

As we purchase additional laptops we will engage with the supplier to arrange secure erasing of all data and disposal in accordance with National Cyber Security Centre standards and through WEEE accredited routes. A certificate of destruction detailing all equipment that has been destroyed will be requested/required as part of the contract. Disconnection from the SG network will be through our shared services agreement with the SPSO.

Assessment and Review

The policies and procedures under this element are subject to ongoing monitoring and review.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Responsible Officers

Corporate Services Manager – Cheryl Glen
Business Support Officer – Joanna Milne

Element 7 – Archiving and transfer arrangements

Records that have enduring value are permanently retained and made accessible in accordance with the Keeper's 'Supplementary Guidance on Proper Arrangements for Archiving Public Documents'.

Statement of Compliance

The SBC File Type Guidance - Retention and Disposal Policy is published on our website. The guidance is based on the Scottish Government's guidance and describes the list of records for which pre-determined disposal dates have been established and the archiving and destruction arrangements that are in place.

The SBC has in place an arrangement to dispose records of archival value with the NRS. The NRS and the SBC are guided by a Transfer Agreement and the NRS had an opportunity to contribute to the SBC records retention schedule through the File Plan which identifies the records selected for permanent preservation. The Retention and Disposal Policy (within the Information Governance Handbook) details the process for transferring records identified by the retention schedule for permanent preservation with the NRS.

Evidence of Compliance

- File Type Guidance - Retention and Disposal
- Transfer Agreement between NRS and SBC
- Retention and Disposal Policy within SBC Information Governance Handbook

Further Developments

Assessment and Review

The policies and procedures under this element are subject to ongoing monitoring and review.

Responsible Officer

Corporate Services Manager – Cheryl Glen

Element 8 – Information security

Records are held in accordance with information security compliance requirements.

Statement of Compliance

The SBC comply with the security and access requirements of the Section 61 Code of Practice: Records Management. Information risks are captured and managed in our Strategic Risk Register, helping ensure that we apply appropriate controls to safeguard information and protect the interests of our stakeholders, while delivering objectives and making the most of opportunities.

The SBC uses eRDM, a system which allows for the secure, audited storage of all electronic documents and records and enforces technological restrictions to prevent unauthorised access, destruction, alteration or removal of records.

Incident reporting arrangements are in place for security incidents and personal data breaches. In the event of a breach, the Commissioner is informed immediately and will coordinate and ensure all the appropriate investigation and reporting processes are undertaken.

To ensure the proper level of security for all records:

- the SBC utilises the secure SCOTS Connect service provided by the Scottish Government to host our network services under an agreed Terms of Supply. Users of the network must be formally registered with an agreed level of access. Access rights of system users who have left are removed immediately
- all employees have met the requirements for receiving a Disclosure Scotland Certificate
- the Commissioner is vetted to Counter Terrorist Check (CTC) by the Scottish Parliament
- all employees undertake security awareness and data protection training
- the building at Bridgeside House, 99 MacDonald Road is adapted to meet the Scottish Government security requirements for the SCOTS network
- the SBC Clear Desk and Screen Policy is described in our Information Governance Handbook and details the procedures to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours
- the SBC Complying with Information Legislation, and Data Protection Policy and Procedure (both within the Information Governance Handbook) detail statutory obligations, guidance for protecting personal data and the emergency protocol for security and data breaches
- the SBC Hybrid Working Policy within the Working for the SBC Handbook describes confidentiality and security rules for business conducted on behalf of the SBC
- the SBC Records Management and Security Guidance: sharing information off-network and out-of-office (within the Information Governance Handbook) details issues that must be considered to ensure that any SBC information worked on out of the office is kept confidential and protected from loss of unauthorised access and exploitation
- Data Protection legislation requirements are covered as part of the induction process with refresher training and other training needs being monitored by Corporate Services Manager

- ICT Handbook Shared Service contains a shared ICT Strategy and IT Security Policy with the SPSO

Evidence of Compliance

- SBC Information Governance Handbook
  - Clear Desk and Screen Policy
  - Complying with Information Legislation
  - Data Protection Policy and Procedure
  - Protective Marking System
  - Records Management and Security Guidance: sharing information off-network and out-of-office
- ICT Terms of Supply
- SBC Hybrid Working Policy within Working for SBC Handbook

Further Developments

Intention to work towards compliance with and certification to Cyber Essentials.

Assessment and Review

This is an area to be examined as part of our Internal Audit services, but all policies and procedures under this element are subject to ongoing monitoring and review.

Responsible Officer

Corporate Services Manager – Cheryl Glen

Element 9 – Data protection

Records involving personal data are managed in compliance with data protection law.

Statement of Compliance

The SBC has a legal obligation to comply with the requirements of the Data Protection Act 2018, ensuring that it has arrangements in place to manage, process and protect personal data. The SBC's Complying with Information Legislation and Data Protection Policy and Procedure details statutory obligations, guidance for protecting personal data and the emergency protocol for security and data breaches. The SBC is legally obliged to protect any personal information that we hold, and we are required to notify the Information Commissioner's Office (ICO).

The SBC is registered with the Information Commissioner as required by the Data Protection Act 1998, registration number ZB298978 (date registered 9 February 2022).

The guide to submitting subject access requests to the SBC is available on our website through our Publication Scheme.

The SBC publishes a privacy notice on our website.

The SBC follows an approach of privacy by design and uses data protection impact assessments (DPIAs) for all projects and activities which involve the handling of personal data and which may have an impact on privacy. We do this in order to help us identify the most effective way of complying with data protection obligations and meeting individual's expectations of privacy.

The SBC has an assigned Data Protection Officer through Officeholder Services.

The SBC outlines its duty to employees in the Managing Personal Data Policy (within our Working for the SBC Handbook).

Evidence of Compliance

- SBC Information Governance Handbook
  - Complying with Information Legislation
  - Data Protection Policy and Procedure
  - Protective Marking System
  - Information Sharing Policy
  - Data Protection Impact Assessments
- Managing Personal Data Policy (Working for the SBC Handbook)
- MoU between SBC and SPCB/DPO
- Website Privacy Notice
- Publication Scheme

Further Developments

We will be developing a stand-alone disposal policy in relation to complaints received against the Code of Practice to ensure all personal data is manually deleted after a 26 month period.

Assessment and Review

The policies and procedures under this element are subject to ongoing monitoring and review.

Responsible Officers

Corporate Services Manager – Cheryl Glen
Business Support Officer – Joanna Milne

Element 10 – Business continuity and vital records

Record recovery, prioritising vital records, is an integral part of the authority's business continuity planning.

Statement of Compliance

The SBC has business continuity arrangements in place to ensure that key systems and services can be recovered as soon as possible in the event of an incident. A Business Continuity Plan has been developed which highlights roles and responsibilities for staff within the SBC but also those organisations where there are shared services. The Plan confirms that the Scottish Government would be responsible for reinstating normal (lost) IT Services in the event of an incident while the SPSO would provide ICT support to the SBC.

The SBC keeps all records in electronic form, which are stored on servers hosted off-site by the Scottish Government, with an agreed back-up schedule as outlined in the ICT SCOTS Connect services Terms of Supply.

Evidence of Compliance

- Business Continuity Plan (redacted)
- iTECS ICT SCOTS Connect services Terms of Supply
- Retention and Disposal Policy within SBC Information Governance Handbook

Further Developments

We look to improve our business continuity planning therefore the current initial Business Continuity Plan is to be reviewed following a comprehensive business impact analysis (BIA) of all SBC functions and activities, which will identify the resources needed to resume business operations within acceptable recovery timeframes. This along with a 'test exercise' is to be concluded following the accreditation of the Corporate Services Manager within Business Continuity.

Assessment and Review

Business continuity documentation will be reviewed annually and BIAs to be developed as and when any new business processes are introduced or following any changes to the strategic priorities of the organisation or its operating environment. The SBC have asked our Internal Audit provider to include business continuity procedures into forthcoming internal audits.

Responsible Officers

Commissioner – Brian Plastow
Corporate Services Manager – Cheryl Glen

Element 11 – Audit trail

The location of records is known and changes recorded.

Statement of Compliance

The Scottish Government's eRDM system, which the SBC uses to manage its strategic, operational and corporate records provides concise audit trails documenting the editing of all records resulting from activities by individuals, systems or other entities. The SBC Business Classification Scheme (as part of Information Governance Handbook) has a section on eRDM which includes management rules and naming conventions.

The SBC operates a paper-less office therefore, there is no central storage or archiving of paper files for any functions.

Evidence of Compliance

- Information Governance Handbook
  - Records Management Policy
  - Business Classification Scheme
  - Data Protection Impact Assessments

Further Developments

Data Protection Impact Assessments are carried out for new systems / procedures involving the processing of personal data.

Assessment and Review

The policies and procedures under this element are subject to ongoing monitoring and review.

Responsible Officer

Corporate Services Manager – Cheryl Glen

Element 12 – Competency framework for records management staff

Staff creating, or otherwise processing records are appropriately trained and supported.

Statement of Compliance

Mandatory training is undertaken by all staff before being granted access to the eRDM system. Guidance and training is available to all staff through the Scottish Government's intranet. Additional training is provided to the Information Management Support Officer (IMSO). The Corporate Services Manager regularly attends PRSA surgeries and webinars on eRDM delivered by the Scottish Government eRDM Team.

Evidence of Compliance

- eRDM training materials
- Scottish Government intranet
- Data Protection e-learning
- Corporate Services Manager job description
- Corporate Services Manager attendance at PRSA surgeries
- Corporate Services Manager attendance at SG-led eRDM webinars
- Business Support Officer job description

Further Developments

Annual Performance and Development appraisals to be conducted which will highlight training gaps and/or opportunities.

Assessment and Review

Completion of mandatory training is monitored.

Responsible Officers

Corporate Services Manager – Cheryl Glen
Business Support Officer – Joanna Milne

Element 13 – Assessment and review

Records Management arrangements are regularly and systematically reviewed with actions taken when required.

Statement of Compliance

The SBC will review the Records Management Plan and all its elements, at least annually but also when any new operational developments occur to ensure that it remains fit for purpose as part of the internal records management processes. The review(s) scheduled in-line with governance meetings, will be led by the Corporate Services Manager using a self-assessment checklist with relevant staff providing input and updates to the sections under their responsibility. The results of the checklist will be shared, actioned and monitored through monthly management team meetings. The monthly and quarterly strategic management meetings include a Governance standing agenda item which includes updates and reviews re policies to be discussed, with any actions being recorded in an action log then discussed/updated at the next meeting.

Any significant changes to any part of the SBC Records Management Plan will be reported to the Commissioner for approval. The updated Plan will then be presented at a forthcoming Advisory Audit Board and the Keeper will be informed of the outcome of any reviews and amendments to the Plan.

Any changes in the supplier of the SG eRDM system would be highlighted to the SBC through our regular meetings with our iTECS Customer Relationship Manager, advance warning would be given along with details on the change taking place and the transition arrangements for the move to a new system. Any updates to the existing eRDM system are communicated to the SBC by our iTECS Customer Relationship Manager and via general communications issued by iTECS.

Evidence of Compliance

- Records Management Policy within SBC Information Governance Handbook
- Governance and Internal Control within Scheme of Governance & Risk Handbook
- Minutes of Monthly and Strategic Management Meetings
- Self-assessment checklist

Further Developments

Assessment and Review

The policies and procedures under this element are subject to ongoing monitoring and an annual review.

Responsible Officers

Corporate Services Manager – Cheryl Glen
Business Support Officer – Joanna Milne

Element 14 – Shared information

Information sharing, both within the Authority and with other bodies or individuals, is necessary, lawful and controlled.

Statement of Compliance

The SBC is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data. The SBC operates in accordance with the Information Commissioner's guidance on data sharing. Data sharing agreements are used to record the specific requirements and circumstances of information sharing and ensure that data is shared fairly and lawfully. When undertaking any new data sharing activities which involve personal information a data protection impact assessment is undertaken to ensure any privacy risks are identified and mitigated.

When required, viewing of personal data held by a third party that cannot be shared over the secure SG network will be viewed on the premises of the third party.

Our Publication Scheme describes what we routinely publish, how and where our documents can be accessed.

Evidence of Compliance

- SBC Information Governance Handbook
  - Information Sharing Policy
  - Data Protection Policy and Procedure
  - Data Protection Impact Assessments
- Data Sharing Agreements
- Website Privacy Notice
- Publication Scheme

Further Developments

Assessment and Review

The policies and procedures under this element are subject to ongoing monitoring and review.

Responsible Officers

Operations Manager – Diego Quiroz
Corporate Services Manager – Cheryl Glen

Element 15 – Public records created or held by third parties

Adequate arrangements must be in place for the management of records created and held by third parties who carry out any functions of the authority.

Statement of Compliance

The SBC has a shared services agreement with the Scottish Public Services Ombudsman (SPSO) which covers HR and employment matters, payroll services, facilities management, financial transaction processing and environmental obligations.

However, no functions of the Scottish Biometrics Commissioner's office is contracted out to third parties, this is confirmed within the Commissioner's statement. The general functions of the Scottish Biometrics Commissioner as described within Section 2 of the Act 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). The Commissioner must lay an annual report on activities each year before the Scottish Parliament and may publish other reports and research, as necessary.

Evidence of Compliance

- Shared Services Agreement
- Commissioner's statement

Further Developments

Assessment and Review

The shared services agreement is reviewed annually by both parties and is audited by both parties through Internal Audit services.

Responsible Officer

The Commissioner – Brian Plastow