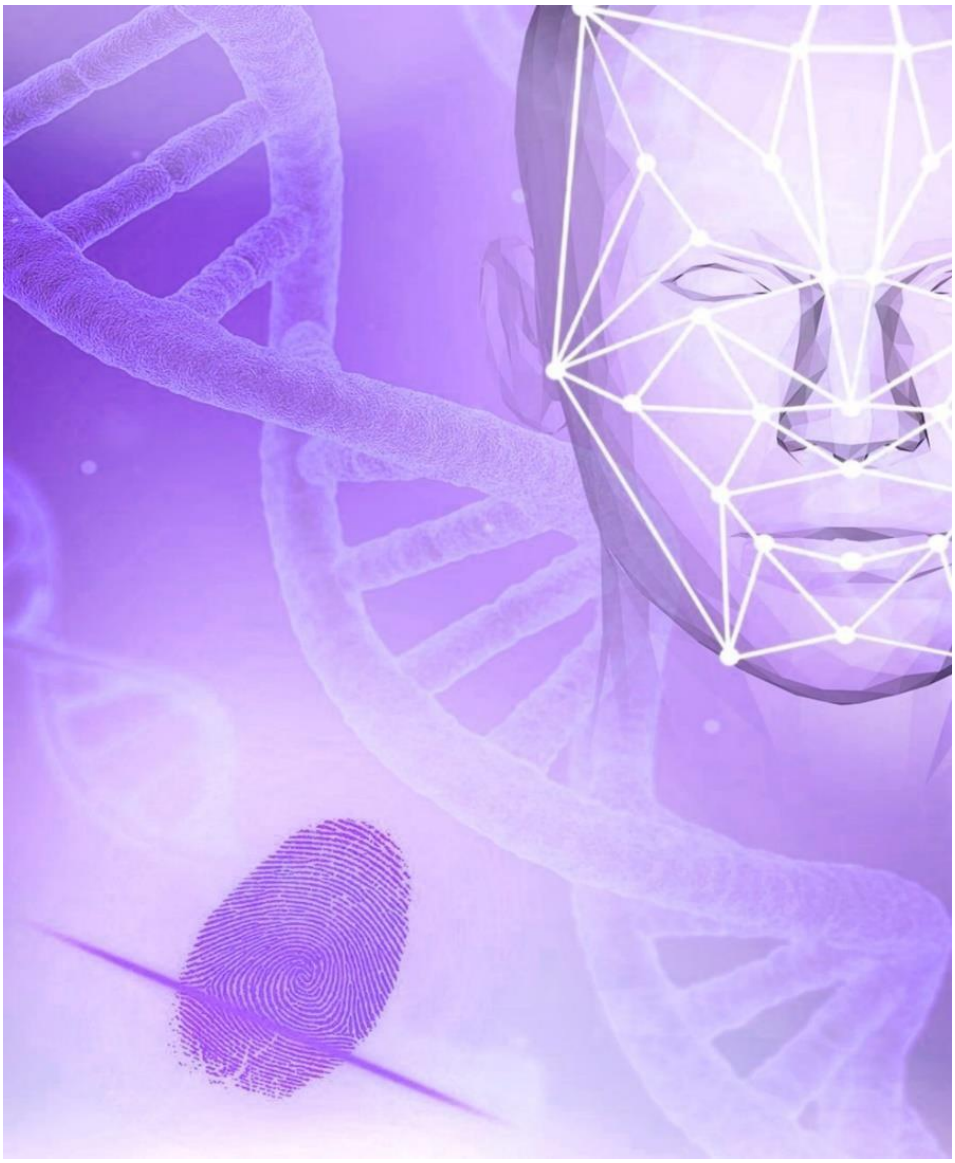
Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

SCOTTISH BIOMETRICS COMMISSIONER

INFORMATION GOVERNANCE HANDBOOK



Safeguarding our biometric future

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Document Control:

Title	Information Governance Handbook
Prepared by	Cheryl Glen
Reviewed by	Dr Brian Plastow
Version Number	2.0
Date	July 2023
Amendments	▪ Additions to text within Information Sharing Policy ▪ Updated hyperlinks added ▪ Additions to text within Records Management and Security Guidance; Information sharing off-network or when out of office ▪ Additions to text within Complying with Information Legislation ▪ Amendments and additions to text within Data Protection Policy and Procedure

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Contents

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Records Management Policy

Introduction

Records management is the professional practice or discipline of controlling and governing what are considered to be the most important records of an organisation throughout the records life cycle, which includes from the time such records are conceived through to their eventual disposal. This work includes identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records.

Records management is part of an organisation's broader activities that are associated with the discipline known as governance, risk and compliance and is primarily concerned with the evidence of an organisation's activities as well as the reduction or mitigation of risk that may be associated with such evidence.

The Scottish Biometrics Commissioner (SBC) recognises that the effective management of its records is essential in order to support our core functions, to comply with legal, statutory and regulatory obligations and to demonstrate transparency and accountability to all its stakeholders. Records are a vital information asset and a valuable resource for the organisation's decision-making processes, policy creation and operations and must be managed effectively from the point of their creation until their ultimate disposal.

Purpose and scope

The purpose of this policy is to demonstrate the importance of managing records effectively within the organisation, to outline key aims and objectives for the SBC in relation to its record-keeping and to act as a mandate for the support and delivery of records management policies, procedures and initiatives across the organisation.

This policy relates to all staff of the SBC and all records created or acquired in the course of its business. It relates to the management of records as an internal facilitative function of the organisation.

The policy is to be read in conjunction with the Records Management Plan for the SBC, which details the current record-keeping practices in place within the organisation.

The aims of this policy include:

- the improvement of business efficiency through less time spent searching for information
- the demonstration of compliance with statutory and regulatory record-keeping obligations including the Public Records (Scotland) Act 2011, the Freedom of Information (Scotland) Act 2002, Environmental Information Regulations 2004 and the UK General Data Protection Regulation and
- the promotion of openness, transparency, accountability and improved corporate governance commensurate with the organisation's role.

The Public Records (Scotland) Act 2011 places an obligation on named authorities in Scotland to produce a records management plan which sets out their arrangements for the effective management of all records. The SBC is a named authority as defined in the Act. The creation of a records management policy statement is a mandatory element of the plan, and is necessary in order to identify the procedures to be followed in managing the organisation's public records.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

What is records management?

Records management (which includes the management of emails) can be defined as the process an organisation uses to manage its records, whether created internally or externally and in any format or media type including emails, from their creation or receipt, through to their destruction or permanent preservation.

Records management is about placing controls around each stage of a record's lifecycle, at the point of creation (through the application of metadata, version control and naming conventions), during maintenance and use (through the management of security and access classifications, facilities for access and tracking of records), at regular review intervals (through the application of retention and disposal criteria), and ultimate disposal (whether this be recycling, archiving, or confidential destruction). By placing controls around the lifecycle of a record, we can ensure they demonstrate the key attributes of authenticity, reliability, integrity and accessibility, both now and in the future.

Through the effective management of the organisation's records, the SBC can provide a comprehensive and accurate account of its activities and transactions. This may be achieved through the management of effective metadata[1] as well as the maintenance of comprehensive audit trail data.

We retain records that provide evidence of our functions, activities and transactions for:

- **Operational Use** – to serve the purpose for which they were originally created, to support our decision-making processes, to allow us to look back at decisions made previously and learn from previous successes and failure, and to protect the organisation's assets and rights
- **Internal and External Accountability** – to demonstrate transparency and accountability for all actions, to provide evidence of legislative, regulatory and statutory compliance and to demonstrate that all business is conducted in line with best practice
- **Historical and Cultural Value** – to protect and make available the corporate memory of the organisation to all stakeholders and for future generations.

Why is records management important?

Information and records are a valuable corporate asset without which we would be unable to carry out our functions, activities and transactions, meet the needs of our stakeholders, and ensure legislative compliance.

The benefits of implementing records management systems and processes include:

- improved information sharing and the provision of quick and easy access to the right information at the right time
- the support and facilitation of more efficient service delivery
- improved business efficiency through reduced time spent searching for information
- demonstration of transparency and accountability for all actions
- the maintenance of the corporate memory

[1] Metadata can be defined in very general terms as 'data about data' and is necessary in order to understand the context, purpose, extent and location of a record. Examples of metadata can include information relating to a record's creator, creation date, receipt date, editor, access history and disposal.

- the creation of better working environments and identification of opportunities for office rationalisation and increased mobile working
- risk management in terms of ensuring and demonstrating compliance with all legal, regulatory and statutory obligations and
- the meeting of stakeholder expectations through the provision of good quality services.

Policy statement and commitment

It is the policy of the SBC to maintain authentic, reliable and useable records which are capable of supporting business functions and activities for as long as they are required. This will be achieved through the consolidation and establishment of effective records management policies and procedures, including:

- the maintenance of a Business Classification Scheme (BCS) to reflect the functions, activities and transactions of the SBC
- the review of the retention and disposal policy to provide clear guidance regarding the management of SBC records and the correct procedures to follow when disposing of business information
- the review of information security policies and procedures in order to protect records and systems from unauthorised access, use, disclosure, disruption, modification, or destruction
- the review of data protection policies in order to demonstrate the SBC's commitment to compliance with the data protection legislation and the safeguarding and fair processing of all personal data held
- the review of the Business Continuity Plan encompassing strategies to ensure vital records held by the SBC remain accessible over time and there are processes in place to monitor the integrity and usability of records
- the identification of records management as a distinct stream within the organisation's training portfolio, with dedicated training provided to all staff
- the completion of a self-assessment review, following the implementation of the records management plan in order to ensure that the records management practices remain fit for purpose and continue to act as exemplars within the profession in Scotland.

Roles and responsibilities

All staff have a responsibility to manage records effectively through the documentation of all decisions and actions made by the SBC; the effective maintenance of records throughout their lifecycle, including access, tracking and storage of records; the timely review of records and their ultimate disposal. All staff are responsible for suitably maintaining all records so that they can be easily retrieved, retaining all records in line with the retention and disposal schedule, ensuring that all actions and decisions are properly recorded and adhere to this policy.

The Commissioner

The lead responsible officer for records management in the SBC.

The SBC Team

All SBC staff are responsible for approving a corporate approach to the management of records as defined within this policy, promoting a culture of excellent record-keeping principles and practices in order to improve business efficiency, supporting records management through commitment and the provision of resources and recognising the importance of preserving the SBC's corporate memory.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Corporate Services Manager

The Corporate Services Manager is responsible for ensuring that records management principles and procedures are established in line with all legal obligations and professional standards, issuing advice and guidance to all staff, and meeting the aims and objectives as outlined in the records management policy.

Legislative framework

The management of the SBC's records is done so in line with the legislative, statutory and regulatory frameworks. Compliance with the policy will facilitate compliance with these acts, regulations and standards.

Relationship to other SBC policies

This policy forms part of the SBC's overall framework but specifically relates to the policies contained within this document (Information Governance Handbook).

Training

A comprehensive training programme is provided to all staff in order to highlight and increase awareness of their responsibilities in line with data protection, freedom of information and records management.

Monitoring and review

The Corporate Services Manager will monitor compliance with this policy and related standards and guidance.

This policy will be reviewed in line with the SBC Records Management Plan, in order to take into account of any new or changed legislation, regulations or business practices.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Business Classification Scheme

Introduction

The SBC has a clear and discrete remit outlined in the Scottish Biometrics Commissioner Act 2020. This is described in more detail on our website.

The SBC recognises that managing documents and in particular electronic documents, presents a significant challenge for an organisation of any size or sector. Electronic record and document management needs to be very carefully considered and structured to ensure the integrity of the documents is not compromised upon capture and they remain retrievable for as long as they are required.

Documentation

All documentation, including corporate records held by the SBC is mostly administrative or supports our legislative function, they are easily defined, highly structured and whose access and retention is clearly determined. Electronic documents are stored on an electronic record and document management system (eRDM).

SBC business classification scheme and file plan

The business classification scheme is modelled on the functions of the SBC, and directly reflects the hierarchical relationship of functions, activities, transactions.

The SBC business classification scheme and file plan is designed to underpin effective electronic documents management by ensuring:

- improved business efficiency through access to documents to enable informed and effective decision making
- structured management of documents retained for legal and regulatory purposes
- accurate capture and management of electronic documents
- retention of a corporate memory of transactions, decisions and actions taken by, or on behalf of, the organisation
- protection of the rights and interests of the organisation (and others) who the organisation retains documents about
- protection of the characteristics of documents, particularly their reliability, integrity and usability and
- identification of documents required for permanent preservation and archive.

Electronic Record and Document Management (eRDM) System

The SBC has adopted the electronic record and document management system (eRDM), as offered on the SCOTS network, to manage the business classification scheme and file plan. eRDM provides a variety of functions including access controls, auditing and disposal using a combination of system and user generated metadata.

The benefits of eRDM to manage the business classification scheme and file plan include:

- determining where a document should be placed in a larger aggregation of documents
- assisting users in retrieving documents

- assisting the responding to requests for information by ensuring only one copy of a document, or location for document exists
- assigning and controlling retention periods and
- assigning and controlling access rights and security markings.

Structure

The structure of the file system is determined by eRDM. This structure conforms to a typical 'functional' filing structure, with three levels of folders that act as segregations for information, representing the functions, activities and transactions. The fourth file level sits beneath these to contain the individual documents. This model is to prevent users from creating idiosyncratic, sub-folder structures below the file level which do not conform to the management rules.

The file level is most critical. It is a type of aggregation or container within eRDM used to store documents and pictures. It is the principal building block of a file plan and the level at which documents are managed through their lifecycle (for example, for disposal or retention).

There are three functions at level four of the business classification scheme – 1) Strategic Planning, 2) Corporate Functions and 3) Operational Functions.

eRDM management rules

Management rules are explicit instructions to users on the preferred means of managing documents within eRDM. These include direction on appropriate capture, access management and disposal of all documents irrespective of format or media.

All documents contained within a single file will have the same access and retention rules applied, regardless of the date they were created.

Retention and disposal guidelines

Open, retention and disposal workflows for the lifespan of each file are controlled by the file type the file was created with. You can find this on our website.

The retention and disposal rules for different activities are outlined in the Retention and Disposal Policy.

File access

The SBC operates the document management system under the values of open and transparent governance therefore, all files are accessible by default to all colleagues and will only be restricted by exception:

- to protect personal data
- to ensure safe and secure financial governance and
- to enforce statutory disclosure restrictions.

Where required, restricted access is applied at the file level of the plan and to specifically named individuals.

Naming conventions

A disciplined approach to naming files and documents is very important, as it greatly assists users with searching and retrieval of the required documentation. Documents are stored in eRDM by an identification

number. This number is used for linking and sharing purposes. The search and browsing feature works best with a maximum of 1000 documents stored within a file.

General guidelines for naming items in eRDM are:

Folders and files:

- files must be titled as specifically and simply as possible, identifying the logical element of the filing structure. This can be achieved by using the following structure: name, description and date. Acronyms should not be used for naming folders or files. However, they can be bracketed after the text is spelled out in full, for ease

Documents:

- name documents consistently and clearly, using a structure that supports the easy location of each document
- each document's name should include a date reference;
- use the shortest name possible, using sentence case with spaces between words to enable the document to be found in the search function
- use the date convention: DD Month YYYY. The order of the name will dictate the order in which the documents are listed therefore, for some groups of documents it may be appropriate to group by common name, with more descriptive names e.g. Animation Procurement 1 / Animation Procurement 2.

eRDM administration

Administration for eRDM is provided by the Scottish Government, including initial set-up of the SBC file plan, application of the retention and disposal rules to each file and the application of access restrictions to each file.

The SBC Information Management Support Officer (IMSO) is a named member of staff with additional administrative rights in eRDM. The IMSO is trained to use the eRDM system.

Document owners have more administration rights over their own documents, such as changing location, than over other documents. Document owners can be changed over the life of the document where required.

SBC IMSO - The Role

The SBC Information Management Support Officer will provide advice on information management to colleagues. They have additional administrative rights and permissions in eRDM.

The IMSO should have a good understanding of business processes and the information needs of colleagues in their area, alongside a strong knowledge of the eRDM system so they can support users.
IMSO tasks will include:

- helping colleagues with their use of My Home and Handy folders
- support file management by creating groups and creating and approving file requests

- managing documents with corporate value or restrictions and checking naming conventions and
- the IMSO also supports new staff in completing their eRDM - introduction for new staff elearning and completing processes for staff who are leaving.

They will be responsible for:

- liaising with Scottish Government with all administration requests including new files and changes workflow rules and access requirements
- reviewing Scottish Government reports for retention and disposal of documents and providing advice on information management to colleagues.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

File Management Guidance

To show good file management it is important that these steps are followed:

- all documents will be filed electronically within eRDM
- documents must not be stored anywhere other than eRDM
- correspondence received by post will be scanned as a PDF then the original will be destroyed. The only exception to this will be if correspondence contains a criminal allegation and may therefore be required in evidence, in these circumstances the original correspondence will be handed over as a 'production' to the relevant investigatory body
- absolutely no complaint paperwork should be kept in email folders, common drives or loose in other locations
- as far as possible, remove and destroy all duplicate copies of documents except for cue cards and contact lists associated with our business continuity arrangements to manage instances of ICT failure
- generally, drafts of letters and reports should not be retained on file – they should be removed when the final version of the letter/report has been agreed. The only exception to this is the draft version of a public report which issued to all parties for comment. We should keep a copy of this electronically to assist in the event that details are questioned or disputed at a later date
- where large volumes of documentation is provided this should be stored in the most appropriate format. Additional documentation should be clearly labelled with our reference number
- when complaints are closed, no further hardcopy documents should be stored, all new documents should be stored on the electronic file only, through scanning if necessary

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Retention and Disposal Policy

Introduction

The SBC recognises that its administrative documents are a unique and irreplaceable resource. The effective management of our documents, regardless of format, is essential in order to support our core functions to comply with legal, statutory and regulatory obligations and to demonstrate transparency and accountability to all its stakeholders. The SBC Records Management Policy sets out a commitment to the implementation of an efficient and effective document management system. Crucial to the success of the policy is the development and implementation of a retention and disposal schedule.

This retention and disposal policy aims to identify documents which should be retained because of their legal, statutory and regulatory obligations, or long-term historical/research value and enable the SBC to dispose of documents promptly when they cease to be of any continuing administrative/legal value.

The policy is to be read in conjunction with the Records Management Policy, which details the importance of managing documents effectively within the organisation, outlines key aims and objectives for the SBC in relation to its recordkeeping and acts as a mandate for the support and delivery of documents management policies, procedures and initiatives across the organisation.

Statutory obligations

The management of the SBC's documents is done so in line with legislative, statutory and regulatory framework. Compliance with this policy will facilitate compliance with these acts, regulations and standards.

Legislative considerations and models of best practice

Freedom of Information (Scotland) Act 2002, Environmental Information Regulations 2004, Data Protection legislation and UK GDPR have provisions entitling individuals to request information that is held by the SBC, but do no oblige the SBC to keep information longer than is required for its purposes.

These Acts therefore, do not determine standard retention periods, although where possible information that has been requested under FOISA, EISR or Data Protection legislation but held by the SBC should not be destroyed until the time allowed for the requestor to request a review and / or appeal has lapsed.

The Scottish Biometrics Commissioner Act 2020 does not determine specific periods for retaining information.

The National Archives and National Records of Scotland have developed Codes of Practice in line with the Freedom of Information (Scotland) Act 2002. In the Records Management: Retention Scheduling, 7. Complaints Records, Section 3.1 states:

'Consider the retention of records relating to complaints in the light of business requirements, taking account of the cost of retention and the use of the records in the future. Very few of these records are likely to be selected for permanent preservation; only those relating to very significant or historical cases are likely candidates.'

The Code requires policies to be in place on Retention, Disposal, Transfer and link to the Business Continuity Plan.

In the absence of prescriptive legislation and regulations, the overriding determinant is what suits the business requirements of the organisation including retention and disposal periods.

Other documents

For administrative functions of the organisation there is legislation which dictates the minimum retention period specific types of record are required to be retained. We have identified legislation which directly impacts on the retention of information we hold. These statutes set minimum timeframes and these have been taken into account when setting our retention timescales.

The SBC creates and receives a variety of documents which are necessary for carrying out the business of the SBC which are subject to more specific controls and regulations than is the case with review documents. Organisations do not have any discretion over the retention period for many types of documents as the legislation dictates the required period.

Those documents where there is discretion, the SBC policy is to retain documents for only as long as there is a business requirement for the record, unless of legal value or historically interest.

Published documents can be found on the SBC website. The SBC website is listed with the NRS web archive whose purpose is to give permanent online access to key websites for future generations and this provides for permanent retention of those documents.

Transfer Agreement with National Records of Scotland (NRS)

The transfer agreement sets out the understanding between the Keeper and the SBC on how the process of depositing, storing and accessing documents of enduring historical, cultural and research value which have been transferred from the SBC to NRS will operate. Deposit of these archival documents in NRS is pursuant to section 5 of the PR(S) Act 1937 and in fulfilment of the SBC'S record management obligations under the PR(S) Act 2011 as also stated in the SBC's published records management policy statement.

Roles and responsibilities

The Commissioner has overall responsibility for ensuring that the SBC complies with the requirements of legislation affecting the management of documents, and with any supporting regulations and codes.

The Corporate Services Manager is responsible for:

- ensuring that the Records Management Policy is implemented effectively
- the provision of record management guidance to staff
- producing procedures documenting all necessary record management arrangements
- regularly reviewing and where necessary amending record management policies and procedure statements and
- making recommendations to the SBC Team in relation to changes or improvements.

All members of staff are responsible for:

- ensuring that the agreed records management policy and procedures are fully observed and implemented within their area of responsibility
- ensuring that all staff within their area of responsibility receive the appropriate training
- documenting their actions and decisions and
- maintaining the documents in accordance with the SBC's agreed policies and practices.

Monitoring and review

The eRDM archiving policy will be reviewed by Scottish Government while the SBC will review their website content, the Records Management Plan and Policy and the File Plan annually or as legislation and/or policy change.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Information Sharing Policy

Introduction
This policy is about sharing information with parties external to the SBC.

IMPORTANT: The SBC Act 2020 Section 16 provides the Commissioner to gather information from those to whom our functions extend. However, Section 19 makes it clear that it is an offence for the Commissioner's office to disclose confidential information.

We need to share information with others to do the jobs under the powers and duties the Scottish Parliament gave us. We will share information with bodies to whom our functions extend e.g. if a data subject complains about a failure by Police Scotland, the Scottish Police Authority or the Police Investigations and Review Commissioner to comply with our Code of Practice. We will also report about our work to the Scottish Parliament and the public. This may include:

- sharing and asking for comments on information we have collected
- publicly reporting our decisions to the Scottish Parliament (reports do not name individuals)
- where our work reveals potential criminal activity, in such circumstances we will share this with the most appropriate investigatory body
- receiving expert advice from someone
- obtaining a translation or providing a translation of information

NOTE: if a complaint or a request for a review is brought to us, we will normally share information with the organisation complained about and if necessary to carry out our function or required by law.

We may also share information for procurements and contracts; when that information shows there may be a risk to someone's health or safety and when that information is important to certain other organisations for their work. The SBC has been given explicit power to share information, this includes:

- Section 3 lists named organisations the Commissioner may work jointly with, assist or consult in the exercise of their functions
- Section 16 states the Commissioner may require information from the organisations to whom our functions extend to ascertain their compliance with the Code of Practice. We would also share information with the Court of Session when we need to report a failure to comply with an information notice as per Section 27 of the Act.

The policy sets out:

- why we share information
- when we can share
- how to identify what information we should share and how to do so securely.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

IMPORTANT: When sharing personal data outside of the SBC secure network, staff must follow the guidance about identifying and using a secure method of transmission set out in the Records Management and Security Guidance: Information sharing off-network or when out-of-office.

Processing personal data

When processing personal data, staff must always comply with the Data Protection principles. These say personal data should be:

- fairly and lawfully processed in a transparent manner
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept for longer than is necessary
- secure and
- the controller must be responsible for, and be able to demonstrate, compliance with the principles.

For organisations with which we share information regularly, we may hold an information or data sharing agreement, that agreement will provide more detail about methods and reasons for sharing but processing should always be in line with the principles. It is important to note that processing personal data to provide anonymised data still needs to meet with the above principles.

Please note in this context, processing includes internal processing of personal information, for example, to analyse data even if the information we then share is anonymised or pseudonymised.

Why we share information

Whenever we are considering sharing personal data or processing personal data to support information sharing we need to identify:

- the purpose or reason for which we are sharing and
- be able to demonstrate that there is a lawful basis in terms of Data Protection legislation for the purposes or reason for which we are sharing.

We have identified it would be suitable to share information for a number of purposes. When identifying these purposes, we have looked at the underlying intent of the legislation that gives us the power to share:

- to support the SBC to more effectively help organisations fulfil their statutory functions, building in best practice and greater efficiency at the point of delivery
- to support reviews that are more efficient by ensuring they are targeted and that organisations have access to all relevant information.

We therefore, consider we may share information when it would achieve those purposes.

We will also share information to:

- protect the health or safety of individuals
- support improvements in the delivery of public services
- support our statutory function
- inform the public and others about our work and the quality of services under our jurisdiction.

In terms of Data Protection legislation we have identified that these purposes meet the following lawful basis:

- performing a task in the public interest
- when we have consent
- the processing is necessary to fulfil a contract that we have with that person
- the processing is necessary for us to meet a legal obligation
- there is a legitimate interest in the processing.

The SBC may hold or process special category data and criminal offence data as described in the next paragraph. Special category data could include information revealing health, ethnicity, religious beliefs etc and criminal offence data – information about criminal convictions and offences and related security measures.

When exercising our duties under Section 15 of the SBC Act 2020 in investigating complaints about potential non-compliance with our statutory Code of Practice, we will exercise an investigatory function in relation to biometric data held by the bodies to whom our functions extend. This may involve us taking possession of special category data. Our interactions would be limited to confirming that such data is held by the body to whom the complaint is directed and confirming with them their legal basis for doing so, and whether the circumstances comply with our Code of Practice.

When investigating a complaint about our Code of Practice, a body to whom our functions extend may cite their lawful basis for retaining biometric data as the data subject having a criminal conviction. Where such information about the existence of a criminal conviction is shared with us, we will not retain this information beyond the point at which our investigation is complete.

Generally we will deal with all complaints we receive however, if a complaint is not for us we will redirect the complainer and have no further involvement.

General enquiries
This guidance does not preclude us from making general anonymised enquiries of other authorities where we feel this is necessary as part of our enquiries and thematic reviews.

The Scottish Biometrics Commissioner Act 2020
Section 3 provides the SBC the power to work with others. If we hold an information sharing agreement with one of those organisations or another agreement that should be followed. The named organisations the Commissioner may work jointly with, assist or consult in the exercise of their functions are:

- The Scottish Parliament
- Scottish Ministers
- The Lord Advocate
- The Chief Constable of the Police Service of Scotland
- Her Majesty's Inspectors of Constabulary in Scotland
- The Scottish Police Authority
- The Police Investigations and Review Commissioner
- The Information Commissioner
- The Commissioner for the Retention and Use of Biometric Material
- The Scottish Human Rights Commission
- such other persons as the Commissioner considers appropriate.

Further to this, Section 16 of the Act states the Commissioner may require information from the organisations to whom our functions extend to ascertain their compliance with the Code of Practice.

We would also share information with the Court of Session when we need to report a failure to comply with an information notice as per Section 27 of the Act.

Where we do not have an agreement we should follow the process below. If we are sharing on a more than occasional basis (i.e. more than once a year or so) we should consider putting an agreement in place. **NOTE:** even where there is a pre-existing agreement, the process is broadly the same.

Confirming that we hold relevant data
SBC may identify that we potentially hold relevant data because of:

- our knowledge and experience of the relevant organisation and its work
- our awareness of public information indicating this is a concern to the organisation
- direct contact from the organisation and
- comments made to us by one of our team.

Before taking any further steps we should test the assumption to see whether that is the case by:

- identifying whether we have a lawful basis for sharing. To do so we need to:
    - confirm the purposes for sharing are covered by the purposes set out in Schedule 5, where we hold an information sharing agreement it may include examples to help us identify these but this assessment should be done on each individual case
- where there is no agreement, before proceeding we should contact the organisation and explain in general terms and without disclosing personal data. We should discuss with them our understanding of the statutory provision to ensure that we are only sharing information that meets their purposes.

NOTE: the decision whether or not to share is one for SBC and we cannot rely simply on a request by a named organisation. We should ensure we understand how the statutory provision covers this request.

All decision about whether or not we hold relevant data should be clearly recorded on file.

Before sharing

Consider individual data rights

While there is reference to the possibility of sharing in these circumstances in our privacy notice, we should proceed on the basis that we will inform data subjects of an intention to release whenever possible.

In addition when the data to be released is special category or a similar type of data, we should also consider whether we should give the data subject the opportunity to make representations before we release data.

We should note and record our reasons for sharing or not with the data subjects and for seeking representations from the data subjects before sharing or not.

When we are sharing special category or other sensitive personal data and are not informing the data subject, we need to take particular care to ensure that we respect the rights of those individuals and actively consider what concerns they may have raised if they had been given the chance to make representations when making our decisions.

Seek assurances about how data will be handled

Seek written (this includes email) assurance from the organisation that they have appropriate measures to retain and process the data in line with our / their obligations. This may be tailored to the specific situation shared but we would anticipate organisations being able to provide evidence that they process information in line with Data Protection legislation, that they have appropriate arrangements for dealing with subject access requests, securing data and dealing with breaches. Where we have an information sharing agreement in place there will be express commitments within that which means we do not need additional assurance in an individual case but note the paragraph below still applies.

Where relevant, if you have identified the data is particularly sensitive you may want to seek specific reassurances to, for example, protect the identify of a third party or a vulnerable person or whistle-blower.

Ensure a secure method for transmission

Identify an agreed secure method to share the information (use the sharing outside of SBC guidance in this handbook which sets out our preferred methods of sharing.

When sharing

Share the minimum amount of data required to meet the purpose. You may be able to identify this from generic discussions with the organisation but the general approach below may be helpful:

- data should be pseudonymised unless doing so means it will not meet the purpose for sharing
- if it is not clear whether or not pseudonymised data will be sufficient, share in a pseudonymised version first. This approach is strongly encouraged when special category or sensitive data is being shared.

Record the decision

As a data controller, the SBC needs to remain accountable for and demonstrate compliance with the Data Protection principles. It is important to record and document decisions. The record should include:

- why we consider the release meets the purposes and any steps taken to confirm this
- decision to inform or not the data subject and, if informed whether we received and considered any representations prior to release
- who made the decision to release e.g. Commissioner and
- the specific details of the information released.

The retention period for the record of the decision to share information should be the same as the information we have released and, unless there are compelling reasons not to, stored in the same file as the information that has been shared.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Records Management and Security Guidance: Information sharing off-network or when out of office

Introduction

The SBC provides secure systems for storing and processing information through the SCOTS network whether that be within the office or working from home. These are referred to in this guidance as the SBC secure work spaces.

This guidance applies to situations where information is shared either physically or electronically outside those secure work spaces. This guidance is intended for all SBC staff.

The SBC as directed by the Commissioner has adopted the following approach**, under no circumstances** must any materials provided to us by Police Scotland, the Scottish Police Authority, or Police Investigations and Review Commissioner (or potentially in the future the National Crime Agency, British Transport Police or the Ministry of Defence Police) that are not already in the public domain be printed off. Additionally, no materials that are 'protectively marked' from any source are to be printed off under any circumstances.

Please see Section 19 of the SBC Act 2020 which creates a specific criminal offence for the Commissioner or SBC staff to knowingly disclose confidential information obtained whilst exercising our functions.

What is the purpose of this guidance?

This guidance gives general advice on the issues you need to consider to ensure that information we process (i.e. hold, work on or share) outside our secure work spaces is kept secure, confidential and is protected from loss or unauthorised access and exploitation. At the same time ensuring that it is accessible to anyone that needs to use it for their work.

It applies to data in all formats, including paper files and documents; electronic data, files and documents; emails; images and video, and sound files.

You must comply with these guidelines to ensure that the SBC meets its duties under Data Protection legislation, Access to Information legislation (ATI, for example, FOISA, EIRs) and the Scottish Public Services Act 2002 confidentiality provisions.

Why is it important to consider data protection and access to information when working outside the SBC secure working spaces?

Data Protection legislation and ATI legislation apply to all paper and electronic data and information, you receive and create as part of your employment/contract with the SBC, regardless of where you work or store it. Data Protection legislation requires the SBC to ensure:

- we hold data about living identifiable individuals for no longer than is necessary
- that personal data is accurate, and
- to adopt security measures for this information to protect it from unauthorised access, amendment or deletion.

More information about our duties and rights can be found in our Data Protection policy and privacy notice.

The UK GDPR and Data Protection Act also gives people the right to access their own personal data that the SBC holds about them while ATI legislation (e.g. FOISA and the EIRs) gives people the right to receive other information that the SBC holds in a recorded, permanent format.

We have a month to respond to a subject access request and 20 working days for FOI or EIRs requests. These deadlines mean that the SBC must know what data and information it holds, and must be able to retrieve that information even if those holding it are away from the office. Section 61 of The Freedom of Information (Scotland) Act 2002 provides for a statutory code of practice on records management which describes the systems we should have in place for managing our information so that we can do this.

How does this affect how I work?
Secure working spaces – have been set up to protect the data we hold electronically and physically. When working outside those spaces, we need to take additional steps to ensure that the data is covered, as far as possible, by equivalent levels of protection.

Step 1: Identifying whether data is being processed
On most occasions it will be obvious you are processing or sharing data outside the secure spaces, for example you will be sending information to an email address that is not part of the Public Services Network (PSN) or physically sending files or documents out of the office. However, the SBC has adopted a paperless office so it should be very rare when files or documents are printed and sent.

Think about where you are working, how and with what data. You can still be in a secure space when you are not physically in the office by working remotely on our network with electronic data, or in a secure physical environment when working with hard copy (Not Protectively Marked) data e.g. when working at home.

But beware! Being in the office does not automatically mean you are in a secure space. Working where there are non-SBC staff and / or contractors present are all examples of non-secure spaces, even in the office. Some very sensitive personal data may need extra security even in the office.

You should always identify whether you are or are not sharing or processing information out with the secure working spaces because if you are you should be asking yourself why, and thinking about what other steps you need to take.

If you are unsure, seek advice before sharing or processing information.

Step 2: Minimise processing or sharing personal data outside the SBC

- When sharing personal data consider:
  - What do I need to share?
  - Why do I need to share it?
  - Have I anonymised / pseudonymised it as much as possible (if not completely)?
  - Could a person(s) still be identified because of the context it is in?

- anonymised data is data that could not be linked to a person without additional information and
- pseudonymised data may contain identifiable information but does not contain names. It provides a layer of protection when compared to including names so should be considered whenever possible.

Complaint reference number and name of organisation should generally be sufficient to identify most complaints without sharing individual names.

When taking personal data out of the office consider:

- do you need to take the personal data out of the office at all?
- always taking personal data securely electronically via a laptop.

The best way to keep data secure is to keep it electronically.

Step 3: Identifying the risk

Loss or damage could result in legal action against you or the SBC; damage to the SBC's reputation; damage to collaborative relationships caused by the inappropriate disclosure of data; or fines from the Information Commissioner's Office. The severity of the impact is closely linked to the sensitivity of the data, whether it is publicly accessible, mitigating actions taken to reduce the risk of loss or theft and the adequacy of policies and procedures. The more sensitive and private the data, the greater the impact of loss is likely to be.

For information that is in the public domain or that we would disclose if asked for it under a FOISA/ EIRs request, the risks are low, and so minimal security measures are likely to be required.

Sensitive information, whether about identifiable individuals or information that would affect the SBC's or another party's business, will require a higher level of security precautions.

For some information the risks are very high. This might include sensitive policing information within documents shared with us by bodies such as Police Scotland to enable us to discharge our statutory functions or information whose disclosure is forbidden by law.

Data in documents / on paper

Information held on paper can leave the office in several ways, including being:

- taken by SBC staff for home working or meetings
- shared for advice or comment
- stolen; and/or
- accidentally included with other documents leaving the office or sent to the wrong address.

Data on paper is vulnerable to loss or unauthorised access in a number of ways. These are some examples, to consider, but it is good practice when taking data out of the office to consider the particular circumstances. Loss may occur:

- as a result of leaving papers in your household (or other office) areas where they may be seen by other members of your household or by visitors. This is most likely to cause difficulties when the information is about identifiable individuals
- as a result of crime, for example, theft of a briefcase
- as a result of loss, particularly while traveling
- as a result of loss or crime in the courier/mail system
- being opened by the wrong person.

Electronic data
Data held electronically is vulnerable to loss or unauthorised access or amendment:

- physically, through the loss, damage or access to the storage medium on which the record is held
- accidentally, for example, if information is stored on a PC or on a shared network where others who do not have permission to see this information have access to the system or you are working in a position where you can be viewed by others
- through technical issues such as a virus, system failure or hardware failure
- as a result of criminal action such as a cyber-attack (for example, such as hacking or deliberately sent virus), or theft of hardware.

Step 4: Protecting the data
Once you have identified and assessed the risk you must take appropriate steps to protect the data.

Data in documents / on paper
If you are physically taking non Police Scotland, SPA and/or PIRC documents home to work for a business need (the printing of protectively marked materials belonging to Police Scotland, SPA or PIRC is prohibited):

- take only what is necessary
- do not take original documents out of the office i.e. where we hold the original version and not a copy
    - if there are exceptional circumstances that make it necessary to take original documents out of the office you must seek the permission of the Commissioner
    - ensure a copy is held in the office either physically or electronically so any loss does not mean the total loss of the data
- transport copy paper files in an SBC authorised locked bag to and from the office. When the documents are not in use, store them in the locked bag until returned to the office
- go directly between locations without putting the bag down in any public place, or leaving it unattended in a vehicle. Take extreme care not to misplace SBC information on the journey to and from work
- if you know you are not going straight home or back to the office you should not take the data out of the office
- ensure others cannot see the information while you are working
- notify the Commissioner and Business Support Officer (BSO) which file documents you are taking off-site and the date they will be returned. The Business Support Officer will keep a record as an audit

trail of the movement of documents out of the office. It is important to sign the document out and back in.

If you are sending documents or receiving documents:

- only send what is necessary
- avoid sending original documents and ensure if this is necessary a copy is held in the office either physically or electronically so any loss does not mean the total loss of the data
- use the SPSO approved courier and
- be clear about who will receive the data: where, when and how. Consider for example:
    - is it a private home or an office where there may be a mail system which means someone other than the recipient may be involved?
    - does it need to be double-bagged or enveloped?
    - should arrangements be made so only the recipient can sign for it and
    - ensure only information that is necessary for the file to get to its recipient is on the outside of the file to prevent it being seen accidentally.

Electronic data

Note: Electronic information is capable of being moved physically as well as virtually. Sending electronic data:

- ensure data is sent to another secure network rather than a personal email
- make clear in the email header if it is confidential and from SBC
- consider using encryption or a password protected workspace. SBC will share details of tools it has access to that can be used to create safer methods of sharing information electronically particularly when the alternative is a personal email
- check your recipient list/addressee BEFORE clicking on send and
- if you have any concerns, take advice before sharing.

If working on a document electronically outside the SBC secure network you should ensure that:

- you limit the amount of information being worked on as far as possible and consider anonymising/pseudonymising the work
- the space you are working in is as secure as possible, for example
    - does it have appropriate security software?
    - is this up-to-date?
    - do you know what network you are linked to?
    - is the network you are linked into secure?
    - are you accessing the network through secure Wi-Fi?
    - can you work outside of the network (i.e. switch broadband and Wi-Fi off)?
    - can you be over-looked?
    - does anyone else have access to the email / workspace you are using and if so can that be limited.
- use passwords on individual documents if they will be stored for any length of time and

- do not store data for longer than is necessary and destroy all copies when the data has been uploaded / sent back to the SBC secure network.

Emergency procedures – 72 hours

Seventy two hours is all the time we have from learning of a data breach to reporting it to the ICO. That includes weekends, out of office, bank holidays, sickness and annual leave. This 72 hour reporting period runs from the time when you first become aware of the breach e.g. if an email containing criminal offence data is sent to the wrong email address the period of reporting the breach runs from when you become aware that the message has been delivered to an unintended recipient. You can take reasonable steps to ascertain whether the message can be recalled before deciding on whether the breach needs to be reported. The ICO have a self-assessment tool which can be used when determining whether a breach should be reported or not. In addition to reporting a breach, we also need to consider whether to notify the data subject of the breach – the test for informing the data subject is higher than for reporting the breach and we need to consider whether it is proportionate to notify the individual having regard to the nature and extent of the breach.

As soon as you are aware of a data loss, or a potential data loss (for example, cannot find a file, even in the office), you must:

- contact the Commissioner immediately or as soon as is practicable. Ideally this should be by telephone, but can be by email if that is the only option
- report exactly what data has been misplaced and under what circumstances this came about. If you use a non-secure email or can be overheard take care not to compound the matter by unintentionally including personal data. Describe the data, rather than repeat it and
- notify the police immediately if there has been a theft, making sure you get an incident number and the name of the officer you spoke to.

Reminder Checklist:

- ☑ Copy document where possible
- ☑ Lockable bag (fireproof for original docs)
- ☑ Password protection
- ☑ Travel arrangements
- ☑ Home storage arrangements

There is a data security checklist when you are considering sharing information outside of the SBC secure workspace.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Clear Desk and Screen Policy

Introduction
Our Act states that we must not disclose information obtained in the course of our work except for purposes set out in the legislation. The SBC is legally obliged to protect any personal information we hold.

Information security is characterised as the preservation of:

- Confidentiality: ensuring that information is accessible only to those authorised to have access
- Integrity: safeguarding the accuracy and completeness of information and processing methods and
- Availability: ensuring that authorised users have access to information when required.

Confidentiality, integrity and availability of information are essential to maintain legal compliance.

Policy statement
This clear desk policy for papers, and a clear screen policy for information processing facilities, are one of many measures to ensure the security and confidentiality of information. Implementing this policy will reduce the risk of unauthorised access, loss of and damage to information during and outside normal working hours.

Clear desk procedure when working in the office
The aim is for all work areas to be cleared of papers at the end of each working day.

- Paper and computer media should be stored in the lockable cabinets and drawers when not in use, especially outside working hours. It is also worth noting that information left on desks is more likely to be damaged or destroyed in a disaster such as fire, flood or explosion
- Lock your cabinets and drawers at the end of each working day and lock the keys in the key cabinet
- A spare copy of team keys will be stored in a keypad operated key cabinet on each floor
- Sensitive or confidential information, when printed, should be cleared from printer immediately

Clear screen procedure

- All computer terminals are password protected
- Computer terminals should be shut down when not in use
- Computer screens should be angled away from the view of unauthorised persons
- The lock (log out) should be set when you leave your desk, automatically set to activate when there is no activity for 15 minutes, and be password protected for reactivation

Training implications
It is essential that all staff are made aware of the key principles of information security. Training on this policy will take place as part of the induction for new starts.

Review / monitoring arrangements
All staff are responsible for monitoring their compliance with the principles/procedures detailed in this policy.

This policy will be continually monitored and will be subject to a regular review which will take place one year from the date of issue and annually thereafter. The review will be carried out by the Corporate Services Manager.

An earlier review may be warranted if one of the following occurs:

- as a result of regulatory / statutory changes or developments
- due to the results / effects of critical incidents and /or
- for any other relevant or compelling reason.

Managerial responsibilities

The SBC has ultimate responsibility for compliance of this policy. SBC staff have the responsibility of developing and encouraging good information handling practice and for ensuring everyone clearly understands and adheres to this policy to help maintain the security and confidentiality of information. All staff have a responsibility for reporting information security incidents including any breaches of confidentiality to the Commissioner.

Non-conformance

There is a requirement for all staff to comply with this policy and where requested, to demonstrate such compliance. Failure to comply will be regarded as a disciplinary incident and will be dealt with under the appropriate policy.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Protective Marking System

Introduction

The SBC holds a wide range of information, some of which is subject to disclosure restrictions and some of which is either currently publicly accessible or to be made available in the future. As an Information Asset Owner and Data Controller the SBC (and in particular the Commissioner) is responsible for this information. Everybody who works for the SBC is responsible for protecting information they work with.

A protective marking system is the method by which the originator of information indicates to others:

- the levels of protection required when handling the information in question, in terms of its sensitivity, security, storage, movement both within and outside the organisation and its ultimate method of disposal
- the severity or impact of the loss or disclosure of the document
- it is designed to protect information from intentional or inadvertent release to unauthorised readers.

Purpose

This guidance is designed to help SBC staff determine when to use additional protective marking on their documents in order to indicate to others the levels of protection required to help prevent the compromise of information.

The protective markings do not impose any specific restrictions on the supply of information under the Freedom of Information (Scotland) Act 2002, the Data Protection Act 2018 or the Environmental Information Regulations 2004.

Protective marking classifications

From April 2014, the Cabinet Office introduced three levels of protective markings - TOP SECRET, SECRET and OFFICIAL. In line with this, the Scottish Government also adopted the three-tier system of classification.

All information the SBC handles meets the criteria for OFFICIAL status only. There is no requirement to mark every document as 'official' as it is understood that this is the default for SBC documents. The risk for 'official' data anticipates that individual hackers, pressure groups, criminals, and investigative journalists might attempt to get information. Any publicly available material is unclassified, including all SBC published reports and material.

With this classification taken as understood, additional marking is used to indicate the nature of the document.

In accordance with the provisions of Section 19 and 20 of the SBC Act 2020, we will not publish materials that are (a) confidential, (b) may be unlawful, (c) might prejudice the administration of justice, or (d) would not be in the public interest. Where we hold such materials, any document will state clearly that it is not suitable for publication and cite the relevant legal exemption.

Determining the level of protective marking

It is the responsibility of the originator to determine when additional protective marking should be applied to the information, based upon an assessment of the sensitivity of its content and the impact of its compromise, often referred to as a harm test. Applying a marking unnecessarily will lead to unnecessary restrictive and expensive controls, which may deny access to those who have a real business requirement or need to know. Conversely, not applying a marking may put assets at risk of compromise since appropriate security controls may not be in place.

Marking information

Complaints re non-compliance with the Code of Practice

On all complaints related correspondence re non-compliance with the Code of Practice, the marker confidential will be included above the address field to indicate the nature of this type of correspondence. The inclusion of a footer to appropriate letters further indicates how the document should be handled.

Meeting Reports

All papers prepared for Monthly Management Team meetings, Advisory Audit Board and Advisory Group will be unmarked i.e. Official unless specifically marked Exempt from Disclosure until finalised. An additional descriptor may be used to describe the reason for the protection or restriction. For example: Restricted – Finance. The use of a descriptor is not mandatory, but they may provide helpful information to users.

Non SBC information

Any material originating outside of SBC that is marked in such a way to indicate sensitivity, for example 'Commercial in Confidence', 'Private' will be handled as indicated.

The SBC in its statutory capacity receives and holds information sent by users which is not protectively marked. Staff must at all times treat this information with confidentiality and must not copy or disclose such information to a third party without prior written approval of the originator.

Emails

If required in an email, protective marking should be added in bold by the sender to the start of the email subject header line and also the top of the body of the email message. This will ensure that all recipients, regardless of what email application they use, will see the sensitivity setting.

Review of markings

Some protective markings will need to be reviewed during the life of the information or document to ensure the marking is appropriate and still relevant.

Carriage of protectively marked assets

Protectively marked or other valuable assets are at risk during transit from accidental or deliberate compromise. To protect such assets when in transit the means of carriage must be reliable, the packaging robust, and the attractiveness, identity and source of the assets concealed under plain cover. Where higher levels of protectively marked assets are involved, a system of audit must be built in to track such assets and to reveal any actual or attempted tampering.

Please refer to the SBC Records Management and Security Guidance. This guidance gives general advice on the issues you need to consider to ensure that any SBC information you work on out of the office is kept confidential and protected from loss or unauthorised access and exploitation, while at the same time ensuring that it is accessible to anyone that needs to use it for their work. It applies to information in all formats, including paper files, electronic data, word-processed documents and emails.

Bulk personal data transmissions

Before bulk data transfer is established with another organisation the following must be considered:

- that there is a valid business requirement to perform bulk data transfers and that it is legal, appropriate and acceptable
- that the recipient where appropriate, is contractually aware of the use that they can make of the personal data SBC provides to them
- that the minimum amount of data is transferred to meet the business requirement and not the entire data set simply because this is the easiest or cheapest option
- that the minimum amount of data is transferred to meet the business requirement and not the entire data set simply because this is the easiest or cheapest option
- that the Public Services Network (PSN) should be the default choice for bulk personal data transfers
- where transfers take place with other external parties the parties should ensure where possible, that contractual and other agreements specify the transfer mechanism and incident management procedures
- where SBC cannot agree or enforce data transfer standards with an external party the risks associated with that transfer must be understood and owned at a senior level.

Incident Reporting

Any incident involving the suspected loss or compromise of any protectively marked material must be reported immediately to the Commissioner and SPCB Data Protection Officer.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Complying with Information Legislation

Requests for Information

The SBC is considered a Scottish Public Authority under the Freedom of Information (Scotland) Act 2002 (FOISA), Environmental Information (Scotland) Regulations 2004 (EIR) and Data Protection Legislation. As such, we must always ensure that we respond to all requests for information in accordance with the statutory requirements of these Acts.

Requests to the SBC for information held (or believed to be held) by the SBC must usually be in writing or some other permanent format. Under the new Data Protection Legislation requests can be made orally.

The SBC aims to acknowledge all information requests within three working days, providing a timescale for responding. It is imperative that all information requests are passed to the IMSO immediately on receipt. Requesters must give an adequate description of the information they require, but do not need to state reasons for the request or refer to relevant legislation. The requester may also express preference for the format for information to be provided in.

Complaint files

Under the SBC Act 2020, Section 19(3) states that it is an offence to disclose confidential information except for a lawful purpose connected with our functions. Releasing this information under FOISA is not one of those circumstances. Therefore, this information is exempt from being released under regulation 10(5)(d) of the EIR and Section 26(a) of FOISA, which is an absolute exemption, therefore we do not need to consider the public interest test. However, they have a right to request information that we hold about them under Data Protection legislation. In light of our duty to provide requesters with advice and assistance, we will consider the request as a subject access request under Data Protection legislation.

During consideration of a complaint for non-compliance with the Code, it is essential that those parties providing information to the SBC are reminded of our obligations under our own Act and under Data Protection legislation; are advised that information could be shared and are invited to provide reasons why any information they provide should not be shared. Where the listed authority has requested that information not be shared with the complainant, the SBC should ask the listed authority to provide a written statement of the reasons for this request. The SBC may decide that the reasons are not sufficient and the final decision ultimately rests with the Commissioner.

Where we have been provided with information that is not relevant to the complaint, we should return it or advise we will destroy it. When recording information, the SBC should use objective language. The SBC should keep in mind that individuals may have a right to see what has been recorded if they request to do so.

Verbal Requests

If the request for information is made verbally, the person dealing with the request should record the request so that the rights under the FOISA, and the EIR will apply. This should certainly be discussed with the requester where there is any doubt whether all the information can be provided. Under the new Data Protection legislation, there is no legal requirement for requests to be in writing, but they must make clear what personal data is being sought. It is a good idea to confirm the request in writing.

Initial handling and recording information requests

Information requests may come in by post, by our online request form, via the front office or direct to SBC staff. All staff should deal with straightforward information requests as far as they can, liaising with the IMSO where appropriate. Where they are unable to deal with the request, they will pass it on to the IMSO.

Where the SBC has simply been copied into correspondence, we should acknowledge receipt but advise that we will not take any further action, and ask the sender not to copy us into correspondence in future.

The person who initially receives the request for information is responsible for recording the request as soon as the request is received and should also copy in the IMSO to make them aware of the request.
Recording the information request via Teams:

- create a new row within the FOI/EIR spreadsheet choosing request type FOI/DP/EIR. The person dealing with the request is the Owner
- all known contact / applicant details should be entered into the spreadsheet and saved
- the type of request, i.e. FOI or DP or EIR, should be selected from the dropdown list, and the request receipt date and request details entered
- information requests are electronic records only. Where letters and paper documents are received, these should be scanned and logged on the electronic record. All emails should be attached to the record within eRDM. File/telephone notes should also be used where appropriate
- when closing the request, the response date, response details, and exemptions should be entered, along with an estimate of the time taken.

Freedom of Information (Scotland) Act 2002

Any person has right to see any kind of recorded information held by a Scottish Public Authority, subject to certain exemptions.

Scottish Information Commissioner

The Scottish Information Commissioner (SIC) is responsible for enforcing and promoting the right to access information held by Scottish Public Authorities. Information and guidance on the Freedom of Information (Scotland) Act 2002 (FOISA), the Environmental Information (Scotland) Regulations 2004 (EIR), exemptions, the public interest test, vexatious/repeated requests, fees/excessive cost of compliance, validity of requests, previous SIC decisions, records management, and much more can be found on the SIC website, which should be the main point of reference. The website also provides many other resources including links to the FOISA, the EIR, Codes of Practice, Fees Regulations and FAQs for public authorities on fees and timescales (including calculation of working days). This SBC guidance document is not intended to be used in place of the SIC guidance, and will not repeat that guidance in detail.

Publication Scheme

All Scottish Public Authorities must produce and maintain a publication scheme which is approved by the SIC. Publication schemes describe the information that the authority publishes, how to access that information and whether it is free of charge or available for a payment. Information in the publication scheme can always be released. There is a chance however, that information which has not yet been uploaded may contain elements that ought not to be released and should be redacted. The SBC publication scheme is available on our website.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Requests for Information
Identity of the requester
Section 8(1)(b) of the FOISA requires that the requester provides their name and an address for correspondence. An email address, or a PO Box would be sufficient contact information to enable the SBC to respond. Requests made on behalf of another person must name the third party (the 'true applicant') in order to be valid.

While the Scottish Information Commissioner deems that an email address is sufficient for the purposes of the FOISA, the Commissioner has issued guidance which states that an applicant must provide his or her own name and address when making a request. The reason for this is that any appeal to the Court of Session in Scotland in connection with a request must be made using the true name of the applicant and this must be the name used in the original request to the public authority.

Broad, general or unclear requests
If the request is too broad or general (for example, seeks all information on a topic over many years), we have a duty to provide advice and assistance to the requester in order to focus the request before either accepting a revised request which meets the criteria or closing the request. The breadth of a request is not in itself an automatic reason to refuse it, although cost considerations might well be relevant here.

The advice is to contact the requester, and ask for clarity about what they are specifically looking for. Section 1(3) of the FOISA and Regulation 9(2) of the EIR deal with the issue of unclear requests and those which have been formulated in too general a manner for an authority to comply.

Mixed EIR / FOISA requests
If a request covers both environmental information and non-environmental information or some of the information is not held, the person dealing with the request must separate out all the elements of the request and deal with each element individually. However, all parts of the request can be dealt with in one letter of response.

Advice and assistance
At all times, SBC must provide advice and assistance to a person who has made, or proposes to make a request for information. This is a statutory duty under Section 15 of the FOISA and Regulation 9 of the EIR. This could include seeking clarification in relation to an information request or assisting the requester in identifying and describing relevant information. If the request is unclear and clarification is sought, the clock does not start until clarification is received.

Assistance to make a request in a recordable format
If the requester is having difficulty making a request in a recordable format, whether because of a disability or any other reason, the person dealing with the request can offer to write it down for them. In such cases, the requester should be asked to sign and return the written request to the SBC. It is appropriate to provide the requester with two copies of the request (one for their records) and a freepost envelope for the reply.

Assistance in framing or clarifying a request
If the requester has had difficulty in stating what information they want, the person dealing with the request can work with them to try to clarify the request into something we can help with or which might be more

useful. The process of seeking clarification must be recorded. The 20 working days for responding to the request will commence on the day after receipt of the clarification. If no clarification response has been received, the person dealing with the request should write to the requester again, stating that we are unable to proceed with the request. Where the information requested is not held by the SBC, the duty to advise and assist includes advising which public authority holds the information requested, if this is known. Where the person dealing with the request does not know which public authority would hold the information, there is no obligation to carry out research on behalf of the enquirer.

Responding to a request

The SBC must establish whether it holds the information requested, consider whether all or part of the information falls within an exempted class, and respond to the request within 20 working days following the date of receipt of the request. For email requests, the received date is the actual date of the email, even if the email is received outside office hours.

Where information cannot be provided, the SBC must issue a refusal notice, stating the reasons for refusal and informing the requester of their rights of appeal. Reasons for refusal include:

- do not hold the information requested (Section 17 of the FOISA)
- information is covered by an exemption
- excessive cost of compliance exceeds £600 (Section 12 of the FOISA) and/ or
- vexatious or repeated request (Section 14 of the FOISA).

Information not held

The requester must be informed that the information is not held, or no longer held by the SBC. The SBC Retention and Disposal Policy may be useful in explaining our procedures for retention, archiving and disposal. In limited circumstances, it may be necessary to issue a refusal letter (Section 18 of the FOISA) which neither confirms nor denies that the information is held by the SBC. The requester must be advised that they have a legal right to request a review of the response and to address any request for review to the Commissioner.

Information held

If the information cannot be supplied straight away, an acknowledgement should be sent to the requester within three working days.

The person dealing with the request must first establish whether we hold the information. This will depend on the information requested and how specific the request is. The person dealing with the request should do some initial searching for relevant information. If unsure of what is held and by whom, the person dealing with the request should issue an email to all relevant staff, setting out the detail of the information request and asking for any relevant information.

For wide-ranging requests involving multiple records, the person dealing with the request should collate the record titles so that a schedule of the documents can be supplied when responding to the request.

The person dealing with the request should also ensure that a record of the searches carried out is available. This may simply consist of the email sent to colleagues and their responses, but where record sets have been searched in more detail, this should be noted.

The person dealing with the request must evaluate all the information identified and reach a view on whether it should be released or withheld under any exemptions, including consideration of the public interest test where appropriate. In some cases, some information may need to be redacted. All information withheld, including redactions, must be explained in the response by citing the relevant exemption and why it has been applied, how the public interest test has been applied, and why the conclusion has been reached that release is not in the public interest.

If a request is being dealt with by somebody other than the Business Support Officer / IMSO, draft refusal responses should be forwarded, along with the information that is to be withheld or redacted, to the Business Support Officer / IMSO for approval before the response is sent out. Where the information can be released in full, it should be collated and if necessary, transferred into the agreed format.

The requester must be advised that they have a legal right to request a review of the response and to address any request for review to the Commissioner.

Charging

The SBC can calculate the estimated cost of complying with FOI requests and may charge within the framework provided by the Freedom of Information (Fees for Required Disclosure) (Scotland) Regulations 2004. We cannot take account of costs incurred in determining whether information is held, or whether the requester is entitled to receive it. The estimate of staff costs cannot exceed £15 per hour. Where the cost of providing information is over £100, the SBC may charge a fee in line with the Fees Regulations. The fee cannot exceed ten percent (£50). Where the cost of providing the information would be over £600, the SBC is not obliged to provide the information under the FOISA. If we do so, we may charge the full cost. In all cases where fees are applied, a fees notice must be issued and must detail how projected costs were calculated. Where the fees will exceed the upper cost limit of £600, requesters must be advised on how to bring their request within the cost threshold.

Common requests for information

Requests for SBC processes or policies

If someone requests information which is available on our website, they should be redirected to the website. This does not need to be dealt with under the FOISA, although we should try to respond within 20 working days in case of appeal to the SIC.

Requests for statistics

These should always be handled under the FOISA, however, some information will be available in the annual reports or on our website. In case of more specific requests where the information has not already been published, SBC staff will collect the relevant information and the Business Support Officer / IMSO will respond to the request.

Requests for legal advice

Section 36(1) of the FOISA states that 'Information in respect of which a claim to confidentiality of communications could be maintained in legal proceedings is exempt information'. In a briefing note explaining this exemption, the SIC confirms that this applies to information shared between a public body and professionally qualified and instructed lawyers. The SBC feels that there is a public interest in maintaining client/lawyer confidentiality where appropriate. However, in the spirit of the FOISA, the SBC might be happy to share the substance of the advice that was received.

Exemptions

Absolute exemptions

Absolute exemptions are listed in Section 2(2) of the FOISA. Some absolute exemptions mean there is no requirement for a harm test or a public interest test under the FOISA (although other rules of law imported into the FOISA by exemptions may contain such tests). Other absolute exemptions cover information that can be accessed through other legislation, for example, subject access requests under Data Protection legislation.

Qualified exemptions

Where a qualified exemption is applied, the SBC must go on to consider the public interest test in order to determine whether the information should be released or could legitimately be withheld.

Public interest test

Although not defined in the FOISA, the public interest has been described as something which is of serious concern and benefit to the public, not just something of individual interest, and as something that is in the interest of the public, not just of interest to the public. When applying the test, public authorities are deciding whether it serves the interests of the public better to withhold or disclose information. The 'public' does not necessarily mean the entire population, but might relate to a relatively localised public, for example, a small community or interest group.

Key exemptions

Section 19 of the Scottish Biometrics Commissioner Act 2020 'Disclosure of confidential information'
Section 26 of the FOISA 'Prohibitions on disclosure'
Section 36(2) of the FOISA 'Confidentiality'
Section 38(1) of the FOISA 'Personal information'
Section 30 of the FOISA 'Prejudice to effective conduct of public affairs'
Section 33 of the FOISA 'Commercial interests and the economy'
Section 36(1) of the FOISA 'Confidentiality'

Vexatious, manifestly unreasonable or repeated requests

The SBC can refuse to comply with a vexatious or repeated request. A vexatious request is determined by the information requested, not the person making the request, and is only relevant to requests made under the FOISA, not Data Protection legislation. An individual can make as many requests for information as he/she wishes, and cannot be labelled as vexatious - each of their requests must be determined on a case-by-case basis. There is no provision for aggregating the cost of responding to multiple requests received from the same person.

Vexatiousness needs to be assessed in all the circumstances of an individual case. If a request is not a genuine endeavour to access information for its own sake, but is aimed at disrupting the work of the SBC or harassing individuals in it, then it may well be vexatious.

There are a number of ways in which it may be possible to identify individual requests as being vexatious, notably:

- if a requester explicitly states that it is their intention to cause the SBC the maximum inconvenience through a request, it will almost certainly make that request vexatious
- if we have an independent knowledge of the intention of the requester. Similarly, if a requester (or an organisation to which the requester belongs, such as a campaign group) has previously indicated an intention to cause us the maximum inconvenience through making requests, it will usually be possible to regard that request as being vexatious
- if the request clearly does not have any serious purpose or value. Although the FOISA does not require the person making a request to disclose any reason or motivation, there may be cases which are so lacking in serious purpose or value that they can only be fairly treated as vexatious. For instance a request for the number of unmarried employees in an organisation, could be classified justifiably as a vexatious request. Such cases are especially likely to arise where there has been a series of requests. Before reaching such a conclusion however, we should be careful to consider any explanation which the requester gives as to the value in disclosing the information which may be made in the course of an appeal against refusal. It would be reasonable to ask why they require the information if it helps you to decide
- if the request can fairly be characterised as obsessive or manifestly unreasonable. These requests will be exceptional and we must have valid reasons for making such a judgement. An apparently tedious request, which in fact relates to a genuine concern, must not be dismissed. However, we are not obliged to comply with a request which a reasonable person would describe as obsessive or manifestly unreasonable. It will obviously be easier to identify such requests when there has been frequent prior contact with the requester or the request otherwise forms part of a pattern, for instance when the same individual submits successive requests for information. Although such requests may not be 'repeated' in the sense that they are requests for the same information, taken together they may form evidence of a pattern of obsessive requests so that we may reasonably regard the most recent as vexatious.

We therefore need to keep records of all FOI's as evidence when assessing potentially vexatious requests. We should contact the SIC for advice before declaring any request to be vexatious.

Formatting information

Responses should be sent by the same means that the request was made. We will comply with the requesters' preference for the format of the information where it is reasonably practical to do so. The Disability Discrimination Act 1995 applies to information requests just as it does to all other service provision. If the requester has specified a format because of a disability, we must comply. The only exception to this is where it would be unreasonable to do so. The burden of proof of what is reasonable lies with the SBC. The Race Relations (Amendment) Act 2000 places similar duties on public authorities in terms of provision of translated information.

Rights of review

If the requester is dissatisfied with the response to an information request, they have the right under Section 20(1) of the FOISA to request a review (and a right of further appeal to the SIC). Requesters must be advised to:

- write to the SBC to request a review within 40 working days of receipt of the decision
- specify their name and address for correspondence
- identify the decision that they wish to have reviewed, or the aspect of the handling of the request that they are unhappy with
- to address their review request to the Commissioner.

Requests for review should be acknowledged within three working days. The review must be an objective assessment of the complaint and involve a thorough assessment of the handling of the request. Reviews will be undertaken and completed as quickly as possible, and in all cases will be completed within the statutory 20 working days.

Rights of appeal

If the requester is dissatisfied with the outcome of the review, they should be advised of their right under the FOISA to appeal to the SIC within six months following the date of receipt of the review notice. It is important that all relevant information, to include information withheld, and any audit trail of decisions taken, is retained until the period for review and appeal to the SIC is complete.

Offences under the FOISA

Where a request has been made and the information would be communicable under the FOISA, it is an offence for any person to take any action with the intention of preventing disclosure of information. This applies to both the SBC and to any person who is employed by, is an officer of or is subject to the direction of the SBC.

Environmental Information (Scotland) Regulations 2004

The Environmental Information (Scotland) Regulations 2004 (EIR) give everyone the right to ask for environmental information held by a Scottish Public Authority. Requests do not need to be in writing, and the 20 working day response deadline can be extended by a further period of up to 20 working days if the volume and complexity makes it impracticable for the authority to deal with the request within the original 20 days. If the request is made in writing, the authority has an obligation to deal with the request under the EIR and an option to also deal with the request under the Freedom of Information (Scotland) Act 2002 (FOISA). However, the authority may choose to apply the exemption in section 39(2) of the FOISA for environmental information, if it is in the public interest to maintain that exemption, and so only deal with the request under the EIR. Review, enforcement and appeals procedures in the EIR mirror those in the FOISA.

Charging

The SBC can charge a 'reasonable amount' under the EIR for environmental information. Where the request is for environmental information which will cost more than £600 to supply, the requester can be asked to pay the full cost of providing the information.

Rights of review

If the requester is dissatisfied with the response to an information request, they have the right under Regulation 16(1) of the EIR to request a review (and a right of further appeal to the SIC). Requesters must be advised to:

- write to the SBC to request a review within 40 working days of receipt of the decision
- specify their name and address for correspondence
- identify the decision that they wish to have reviewed, or the aspect of the handling of the request that they are unhappy with
- address their review request to the SBC Commissioner.

Requests for review should be acknowledged within three working days. The review must be an objective assessment of the complaint and involve a thorough assessment of the handling of the request. Reviews will be undertaken and completed as quickly as possible, and in all cases will be completed within the statutory 20 working days.

Rights of appeal

If the requester is dissatisfied with the outcome of the review, they should be advised of their right under regulation 17 of the EIR to appeal to the SIC within six months following the date of receipt of the review notice. It is important that all relevant information, to include information withheld, and any audit trail of decisions taken, is retained until the period for review and appeal to the SIC is complete.

Data Protection Legislation

The Information Commissioner's Office (ICO)

The SBC is legally obliged to protect any personal information that we hold and we are currently registered as a data controller with ICO (Registration Number: ZB298978; Date Registered: 10 February 2022). The ICO is there to help organisations understand their obligations and keep them updated as and when they change. Information and guidance on all areas of Data Protection and our responsibilities can be found on the ICO website, which should be the main point of reference.

If an individual believes there has been a breach of the Data Protection legislation they can ask the ICO to assess whether our processing of personal data complies with the legislation. The ICO can ask us to take steps to comply with the legislation, issue enforcement notices and even impose financial penalties in respect of deliberate or reckless handling of personal data which seriously breaches the legislation.
The ICO cannot award compensation, only the courts can do this.

Data protection audit

The ICO may make an assessment as to whether an organisation's processing of personal data follows good practice. Following completion of the audit, the ICO will provide a comprehensive report to the organisation along with an executive summary, which is published on the ICO website with the data controller's agreement. Organisations can register their interest with the ICO on their website to be considered for a data protection audit.

Data controller
A data controller is a person who determines the purpose for which and the manner in which any personal data are, or are to be, processed. The SBC is a data controller.

Processing
Processing means obtaining, recording, or holding the information or carrying out any operation or set of operations on it, including:

- organisation, adaptation or alteration
- retrieval, consultation or use
- disclosure by transmission, dissemination or otherwise making available and
- alignment, combination, blocking, erasure or destruction.

Data Protection principles
Data Protection legislation works in two ways. Firstly, it helps to protect individuals' interests by obliging organisations to manage the information they hold in a proper way. It states that anyone who processes personal data must comply with the Data Protection principles, which make sure that it is:

- fairly and lawfully processed in a transparent manner
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept for longer than is necessary
- secure and
- the controller must be responsible for, and be able to demonstrate, compliance with the principles.

The second area covered by Data Protection legislation gives individuals important rights, including but not limited to the right to know what information is held about them and the right to correct information that is wrong.

Correcting Information
If individuals believe the personal data that we hold is inaccurate, they can write to us to tell us what they believe is wrong with their information and what should be done to correct it.

If a member of the public is concerned about our information rights practices, where they felt inaccurate information was contained within our file, we the organisation are responsible to deal with this, to put right anything that's gone wrong.

The Data Protection legislation imposes obligations on us to ensure the accuracy of the personal data we process. We must comply with these provisions by:

- taking reasonable steps to ensure the accuracy of any personal data we obtain
- ensure that the source of any personal data is clear
- carefully consider any challenges to the accuracy of information and
- consider whether it is necessary to update the information.

A concern in the content of a document can be someone else's opinion, opinions are naturally subjective and can depend on the understanding and experiences of the individual concerned. The fact that someone else might hold a different opinion does not make the first opinion inaccurate. A view expressed by the complaints reviewer is a statement of opinion rather than fact and a difference of opinion may not constitute inaccurate information we hold.

Preventing processing of information

Individuals can also ask the SBC not to process information about them that causes substantial unwarranted damage or distress. A response must be provided within one calendar month. The SBC is not always bound to act on the request. Link to SBC Data Protection Policy and Procedure. This approach is known as the right to object to the processing but the existence of these rights depend on the purposes and legal basis of the processing used by the SBC. For example, the right to object to processing will not apply when the SBC are processing personal data for the purposes of a legal obligation to which the data controller is subject e.g. in relation to the statutory requirement to investigate complaints under the Code of Conduct.

Processing subject access requests

One of the main rights which Data Protection legislation gives to individuals is the right of access to their personal information. As a data controller, the SBC is required to respond to Subject Access Request (SAR)'s under Data Protection legislation.

Consultation

Relevant SBC staff will be asked for any comments they may have about information before it is released. Where information has been provided to the SBC by third parties, it may be appropriate to ask for any comments from those third parties before it is released, especially where sensitive personal information is concerned. This is particularly important where the release of such information without a third party's prior consent may result in an actionable breach of confidence. However, consultation should always be proportionate. The consultation letter should set out the parameters of the consultation and make it clear that it is ultimately a matter for the SBC to decide whether the information should be released. The letter should give a date by which responses must be made, allowing time to formulate the response to the requester. In the case of medical records, comments must be obtained from the relevant health professionals as soon as possible.

Repeat requests

We are not obliged to comply with an identical or similar request to one we have already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones. SBC practice is that a minimum of 12 months should have elapsed between the first request and receipt of the second. If the requester disputes our definition of a 'reasonable interval' in respect of their request, they may complain to the ICO.

Conjoined data

The SBC may withhold information if it contains personal data of another individual who can be identified from that information, unless the other individual consents, or it is reasonable not to get consent. Information does not have to be released unless it is reasonable to release it taking into account the tests in Data Protection legislation. Redaction should be considered in these circumstances. Disclosing third party

personal data without a valid reason constitutes a breach of Article 8 of the European Convention of Human Rights.

SBC Complaints re Code of Practice
Information relating to on-going complaints is likely to be more sensitive than information from a closed complaint, but in either situation it is important to consider whether disclosure would have any adverse consequences, either for the SBC or for other parties. Responses to such requests should always be discussed with the Commissioner.

Exemptions
Data Protection legislation sets out the exemptions which may be used to withhold information from data subjects. Some exemptions to the subject access provisions include:

- confidential references given by the data controller
- information relating to negotiations with the data subject
- self-incrimination.

Subject access appeal
Individuals can appeal to the ICO if they consider the SBC has not complied with Data Protection legislation. If an individual is unhappy with the SBC response, or the way in which their request has been handled, the matter should be referred to the ICO. In case of appeal to the ICO it is SBC practice to retain all relevant information for six months.

How to deal with specific types of requests
Requests for copies of documents originally sent to us
If complainants send us original documents, we will normally take copies for our records and return the originals as a matter of course. Any request for their own information should be handled the same way, we do not need to handle this as a formal SAR request although we should try to respond within 20 working days, to avoid any appeal to either Information Commissioner.

Requests for copies of Compliance Notices
We will always publish our Compliance Notices on our website.

Requests after a report is laid
Normally, the publication of a report signifies the end of an debate we can enter into about the complaint. However, complainants are still entitled to request information following the report. If we receive correspondence which may be a request for information, staff should refer to the Business Support Officer / IMSO for advice. Generally there will be a difference between a request for information (for example, question starting who, when, what, where) and a question about our handling of the complaint (for example, a question starting how or why) however it will not always be as clear-cut as this.

Requests for service delivery complaint information
Service delivery complaints are a separate process to handling complaints about non-compliance with the Code. Where staff have commented on the representations made against them, we maintain that the free and uninhibited provision of information by the Complaint Reviewer is an essential part of investigating this

kind of complaint, and that the member of staff concerned should be entitled to a degree of confidentiality. We reserve the right to withhold this kind of information from the complainant.

External guidance
The ICO guidance The ICO has developed guidance to assist in complying with Data Protection legislation. This very useful guidance can be found on their website.

Scottish Ministers' Section 60 Code of Practice on the discharge of functions by Scottish Public Authorities under the Freedom Of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004
Under Section 60 of FOISA and Regulation 18 of the EIR, Scottish Ministers may publish a Code of Practice which describes the practice which they consider would be desirable for Scottish Public Authorities to follow in connection with the discharge of their functions under FOISA and the EIR. This can be found on the Scottish Government website.

This guidance stresses in particular the best practice to be followed in providing advice and assistance to requesters, and promotes the importance of proactively publishing information.

Scottish Ministers' Section 61 Code of Practice on Records Management by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002
Under Section 61 of FOISA, Scottish Ministers may publish a Code of Practice (the Code) which describes the practice which they consider would be desirable for Scottish Public Authorities to follow in connection with the keeping, management and destruction of the authorities' records. The Code of Practice is available on the Scottish Government website.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Data Protection Policy and Procedure

Scope of policy
This policy applies to all staff employed by the SBC on a permanent, fixed-term or temporary contract.

This policy applies to all situations where we process (collect, store, use, share) personal data about living individuals. It includes, but is not limited to information processed electronically, on paper, in emails, in employee files, in internal memos, in photographs and on audio equipment. Individuals may include for example current, past and prospective employees, customers, advisers and others with whom we communicate.

See separate policy specifically for managing SBC employee personal data – SBC Managing Personal Data in the Working for SBC Handbook.

Purpose of policy
The SBC processes (collects, stores, uses, shares) personal data about living individuals as part of our operational activities and has a duty to ensure this processing is in accordance with legal requirements. The main legislative requirements are in the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

The SBC recognises the importance of privacy by design and the correct and lawful treatment of personal data.

The purpose of this policy is to enable SBC to:

- establish a framework for the processing of personal data (regardless of format) which ensures we meet all our responsibilities and safeguards the rights of the individuals
- comply with the law in respect of the data it holds about individuals
- follow good practice
- protect SBC's staff and other individuals and
- protect SBC from the consequences of a breach of its responsibilities.

Staff will be provided with guidance, training and procedures to aid compliance with this policy.

Data protection fee
The SBC must pay the ICO an annual Data Protection fee. The SBC have a current registration under the Act and falls within tier 2: small and medium organisations.

Brief introduction to Data Protection Legislation
The SBC is committed to compliance with the requirements of the UK GDPR and the DPA (Data Protection Legislation). The Data Protection legislation establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

Data Protection principles

All personal data will be processed (obtained, used, shared, handled, transported, stored) in accordance with the Data Protection principles set out in the Data Protection legislation. Article 5 of the UK GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that the controller shall be responsible for and be able to demonstrate compliance with the principles.

Satisfaction of principles

In order to meet the requirements of the principles, the SBC will:

- observe fully the conditions regarding the fair collection and use of personal data
- meet its obligations to specify the purposes for which personal data is used
- collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements
- ensure the quality of personal data used
- apply strict checks to determine the length of time personal data is held
- ensure all the rights of individuals can be fully exercised
- take the appropriate technical and organisational security measures to safeguard personal data (from accidental destruction, theft or any other loss)
- put appropriate Data Protection measures in place throughout the entire lifecycle of our processing operations and
- maintain documentation of our processing activities.

In addition, SBC will ensure that:

- a Data Protection Officer within SPCB continues to provide support and advice
- everyone managing and handling personal information understands that they are contractually responsible for following good Data Protection practice
- everyone managing and handling personal information is appropriately trained to do so
- processors are compliant with Data Protection legislation
- anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do
- queries about handling personal information are promptly and courteously dealt with
- methods of handling personal information are regularly assessed and evaluated
- performance with handling personal information is regularly assessed and evaluated
- privacy by design is satisfied and Data Protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests are carried out
- privacy information is provided to individuals, regularly maintained and updated
- we have suitable accountability processes in place and can provide auditable tracking of processing
- the lawful basis for processing is understood and can be applied to all processing
- where personal data has to be taken off-site, documented procedures will be in place to mitigate against any loss
- personal data is not transferred abroad without suitable safeguards.

Record of processing
We will maintain records on several things such as processing purposes, data sharing and retention and will make the records available to the ICO on request. In particular, we document the following information:

- the name and contact details of SBC and our Data Protection Officer
- the purposes of our processing
- details of any transfers to third countries including documenting the transfer mechanism safeguards in place
- retention schedules
- a description of our technical and organisational security measures.

Personal data
This policy applies to information relating to identifiable individuals. This includes any expression of opinion about the individual and any indication of the intentions of the SBC or any other person in respect of the individual.

Personal data is defined as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.'

This definition provides for a wide range of personal identifiers to constitute personal data, including:

- name, identification number, location data or online identifier or
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

The Data Protection legislation applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised for example, key-coded - can fall within the scope of the Data Protection legislation depending on how difficult it is to attribute the pseudonym to a particular individual.

The types of personal data that the SBC may process include information about: current, past and prospective employees; complainants, applicants, aggrieved individuals and interested parties; suppliers and others with whom SBC communicates. This personal data whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection legislation.

Special category data and criminal offence data
The UK GDPR defines special category data and criminal offence data as follows:

Special category data:

- personal data revealing racial or ethnic origin
- personal data revealing political origins
- personal data revealing religious or philosophical beliefs
- personal data revealing trade union membership
- genetic data
- biometric data (where used for identification purposes)
- data concerning health
- data concerning a person's sex life
- data concerning a person's sexual orientation

Criminal offence data:
The UK GDPR gives extra protection to 'personal data relating to criminal convictions and offences or related security measures'. This covers a wide range of information about offenders or suspected offenders in the context of:

- criminal activity
- allegations
- investigations
- proceedings

It includes not just data which is obviously about a specific criminal conviction or trial, but may also include personal data about:

- unproven allegations
- information relating to the absence of convictions

It also covers a wide range of related security measures, including:

- personal data about penalties
- conditions or restrictions placed on an individual as part of the criminal justice process
- civil measures which may lead to a criminal penalty if not adhered to

It does not cover information about other individuals, including victims and witnesses of crime. However, information about victims and witnesses is likely to be sensitive, and controllers should take particular care when processing it.

Given the sensitivity and risks to processing special category and criminal offence data we can only do so if we have a condition for processing with a basis in UK law.

We process special category and criminal offence data for the purposes of investigating complaints made to us as part of our statutory function in terms of Section 15 of the Act. In these circumstances the applicable condition for processing of special category data is in terms of Article 9(2)(g) of the UK GDPR where '*processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*'.

For criminal offence data the condition for processing is in terms of Article 10 of the UK GDPR where '*processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member state law providing for appropriate safeguards for the rights and freedoms of data subjects'.*

The substantial public interest condition we rely on to process special category and criminal offence data in these circumstances is in terms of paragraph 6(2)(a) of Part 2 to Schedule 1 of the Data Protection Act 2018 where processing is necessary for the exercise of a function conferred on a person by enactment or rule of law.

Where special category and criminal offence data is processed by the SBC we carry out the following steps:

- we document the condition for processing we rely on in the DPIA in our privacy notice
- we document the lawful basis for our processing in our privacy notice
- we retain and erase the personal data in accordance with our retention and disposal policy

Individual rights
The Data Protection legislation provides the following rights for individuals (subject to exemptions):

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure

- the right to restrict processing
- the right to data portability
- the right to object and
- rights in relation to automated decision making and profiling.

Individuals also have the right to withdraw consent where given, and the right to complain to the ICO. Any requests to exercise these rights are forwarded to the Business Support Officer / IMSO for advice.

Policy statement
SBC recognises that its first priority under the Data Protection legislation is to avoid causing harm to individuals. In the main this means:

- keeping information securely in the right hands, and holding good quality information.

Secondly, the Data Protection legislation aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account.

SBC fully endorses and adheres to the principles of Data Protection as set out in the Data Protection legislation and will ensure that it treats personal information lawfully and correctly. SBC will:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- be accountable and demonstrate compliance
- take responsibility for complying at the highest management level and throughout the SBC
- provide training and support for staff who handle personal data, so that they can act confidently and consistently.

Key risks
The Information Commissioner identifies the main risks where non-compliance with the Data Protection principles may result in damage to both individuals and the organisation:

- a failure to identify and implement controls by which compliance with Data Protection can be measured and reported, raises the risk of the 'data controller' being unaware of whether it is meeting its obligations, resulting in poor Data Protection practice or potential breaches of the Data Protection legislation not being identified or addressed
- a failure to provide and implement staff training and awareness regarding the correct use and management of personal records raises the risk of loss or inappropriate usage of data, with the potential to cause damage and distress to individuals, and reputational damage to the 'data controller'
- a failure to implement security measures which adequately protect electronically held personal data raises the risk of loss, damage or inappropriate access to data leading to distress to the affected individuals, reputational damage to the 'data controller' and non-compliance with the Data Protection legislation

- a failure to appropriately control and secure manual personal data both within and outside the 'data controller's' premises raises the risk that personal data will be lost, damaged or inappropriately disclosed, resulting in distress to the individual and non-compliance with the Data Protection legislation
- a failure to ensure Subject Access Requests are dealt with appropriately raises the risk that an individual's rights to information may be compromised resulting in distress to the individual and non-compliance with the Data Protection legislation.

SBC has identified the following potential key risks, which this policy is designed to address:

- breach of confidentiality (information being given out inappropriately)
- insufficient clarity about the range of uses to which data will be put, leading to data subjects being insufficiently informed
- failure to offer choice about data use when appropriate
- breach of security by allowing unauthorised access
- harm to individuals if personal data is not up to date
- insufficient clarity about the way personal data is being used
- inadequate data processor contracts.

Data protection Impact Assessments
A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project. We must do a DPIA for processing that is likely to result in a high risk to individuals. This includes some specified types of processing. It is also good practice to do a DPIA for any other major project which requires the processing of personal data. We can use the ICO screening checklists to help decide when to do a DPIA.

Our DPIA must:

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks.

To assess the level of risk, we must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. We should consult our Data Protection Officer and where appropriate, individuals and relevant experts. Any processors may also need to assist us. If we identify a high risk that we cannot mitigate, we must consult the ICO before starting the processing. The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, they may issue a formal warning not to process the data, or ban the processing altogether.

Further guidance
Further detailed data protection guidance is available on the ICO website.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Annex 1

Responsibilities, training and non-compliance actions

The SBC Team	All staff regard the lawful and correct treatment of personal information as of vital importance to successful operations, and to maintaining confidence between the SBC and those with whom we deal
Commissioner	The Commissioner has overall responsibility for ensuring compliance with the current applicable legal framework and ensuring that all personal data held by the SBC is managed in accordance with the law and internally adopted standards, policies and procedures The Commissioner has the role of arbiter in respect of Data Protection complaints received. The Commissioner will oversee an investigation, review any decisions and report six-monthly to the Advisory Audit Board on the number and outcome of DP complaints
Data Protection Officer (DPO)	We have a duty to appoint a DPO. The Scottish Parliament Corporate Body (SPCB) shares the services of its DPO with the SBC. The MoU between the SBC and the SPCB gives details about the service, including DPO accessibility
Corporate Services Manager (CSM)	The CSM has the following operational responsibilities: ▪ briefing SBC management team on Data Protection responsibilities ▪ reviewing Data Protection and related policies, guidance and procedures ▪ ensuring that Data Protection induction and training takes place ▪ coordinating subject access requests and other Data Protection requests/ concerns ▪ developing policy, procedures and guidance in respect of Data Protection legislation ▪ supporting all members of staff to comply with their obligations under the legislation ▪ issuing guidance The CSM is responsible for maintaining this policy. For any questions about this policy, or to report misuse of corporate or personal data, please contact the CSM
All staff	All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work and to be fully aware of their duties and responsibilities under the Data Protection legislation. All employees are responsible for:

	▪ familiarising themselves with the implications of Data Protection in their job ▪ adhering to this policy and supporting guidance ▪ reporting any activities that do not comply with this policy ▪ seeking guidance and advice where necessary ▪ checking that any personal data that they provide is accurate and up to date ▪ informing the SBC of any changes to information which they have provided, for example, changes of address ▪ checking any information that the SBC may send out from time to time, giving details of information that is being kept and processed

Staff training and acceptance of responsibilities

Induction	All staff who have access to any kind of personal data will have their responsibilities outlined during their induction procedures
Continuing training	The Data Protection legislation requires us to ensure that anyone acting under our authority with access to personal data does not process that data unless we have instructed them to do so. It is therefore vital that our staff understand the importance of protecting personal data, are familiar with our security policy and put its procedures into practice Compulsory Data Protection training is provided annually. We will provide further opportunities for staff to explore Data Protection issues through training, including our responsibilities as a data controller under the Data Protection legislation Staff should be aware of their responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority
Staff acceptance	This policy will be available to all staff

Non-compliance actions

Enforcement	Employees found to be in violation of this policy by either unintentionally or maliciously stealing, using or otherwise compromising corporate or personal data will be subject to disciplinary action under SBC's disciplinary procedures Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with their line manager or the SPSO HR Officer in the first instance

Monetary penalties	The Information Commissioner can serve notices requiring organisations to pay for serious breaches of the Data Protection legislation. In brief, the Commissioner may impose a monetary penalty notice if a data controller has seriously contravened the Data Protection principles and the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the data controller must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it
Offences under the Act	It is an offence to knowingly or recklessly: ▪ handle personal data without the consent of the controller; ▪ procure or disclose the personal data of another person without the consent of the controller; ▪ retain personal data, after it has been obtained, without the consent of the person who was controller when it was obtained; ▪ re-identify de-identified personal data without the consent of the controller who de-identified the personal data; and ▪ process personal data that has been re-identified (which was an offence), without the consent of the controller responsible for the de-identification It is also an offence: ▪ to sell, or offer to sell personal data that has been unlawfully obtained, which includes advertising this data for sale; ▪ where an access or data portability request has been received, it is an offence for a controller or related persons, including a processor, to obstruct the provision of information which an individual would be entitled to receive; ▪ to require another person to request access to a relevant record (includes a health record and records relating to a conviction or caution). Such a request is not permitted in connection with recruitment or continued employment of an employee or a contract for services; and ▪ if a person requires another person to make an access request as a condition of providing goods, facilities or services to them or another (which are provided to the public or a section of the public) Defences of the above offences are detailed in the Data Protection legislation

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Annex 2

Confidentiality

Scope	Confidentiality applies to a much wider range of information than Data Protection. Please refer to the Terms and Conditions of Employment, and the Working for the SBC Handbook – particularly Conduct and Behaviour and Working from Home policies
Understanding of confidentiality	When working for SBC, staff will often need to have access to confidential information which may include, for example: ▪ personal information about our customers ▪ information about the internal business of SBC ▪ personal information about colleagues working for SBC SBC is committed to keeping this information confidential, in order to protect people and SBC itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. Staff must use only the information they have been authorised to use, and for purposes that have been authorised. Staff should also be aware that under Data Protection legislation, unauthorised access to data about individuals is a criminal offence Staff must assume that information is confidential unless they know that it is intended by SBC to be made public. Staff must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular staff must: ▪ not compromise or seek to evade security measures (including computer passwords) ▪ be particularly careful when sending information to other parties ▪ not gossip about confidential information, either with colleagues or people outside SBC ▪ not disclose information, especially over the phone, unless they are sure that they know who they are disclosing it to, and that they are authorised to have it If staff are in doubt about whether to disclose information or not, they must not guess. Staff should withhold the information while they check with an appropriate person whether the disclosure is appropriate Confidentiality obligations continue to apply indefinitely after staff have stopped working for SBC

Communication with data subjects	SBC have privacy information for data subjects, setting out how their information will be used. This will be provided when appropriate, available on request, and on the SBC website
Authorisation for disclosures not directly related to the reason why data is held	Where anyone within SBC feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done with consultation of the Commissioner. All such discussion and disclosures will be documented

Security

Scope	This document defines the data security policy of the SBC. The SBC takes the privacy of our employees and service users very seriously. To ensure that we are protecting our corporate and functional data from security breaches, this policy must be followed and will be enforced to the fullest extent The goal of this policy is to inform employees at the SBC of the rules and procedures relating to data security compliance This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that: ▪ any personal data which they hold is kept securely; and ▪ personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party Data Protection legislation states 'Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk'. The SBC must ensure the 'confidentiality, integrity and availability' of our systems and services and the personal data we process within them. We must ensure that:

	▪ the data can be accessed, altered, disclosed or deleted only by those we have authorised to do so (and that those people only act within the scope of the authority we give them); ▪ the data we hold is accurate and complete in relation to why we are processing it; and ▪ the data remains accessible and usable, i.e., if personal data is accidentally lost, altered or destroyed, we should be able to recover it and therefore prevent any damage or distress to the individuals concerned
Specific risks	The SBC has identified the following risks: ▪ information passing between the SBC and those to whom our functions extend could go astray or be misdirected ▪ processing of sensitive and confidential information - potential damage and distress if compromised ▪ staff with access to personal information could misuse it ▪ staff could continue to be sent information after they have stopped working for SBC if their records are not updated promptly ▪ poor website security might give a means of access to information about organisations once individual details are made accessible online ▪ staff may be tricked into giving away information, either about complainants or colleagues, especially over the telephone, through 'social engineering'; processing information off network and out of office; and email
Data types	The SBC deals with one main kind of data: ▪ information processed in connection with our functions under the Scottish Biometrics Commissioner's Act 2020
Data classifications	The SBC business classification system is modelled on the functions of the organisation. See Business Classification policy All information the SBC handles meets the criteria for OFFICIAL status only. Protective marking guidance helps SBC staff determine when to use additional protective marking on their documents in order to indicate to others the levels of protection required to help prevent the compromise of information
Security measures	SBC utilises the secure SCOTS Connect service provided by the Scottish Government to host our network services under an agreement. Users of the network must be formally registered with an agreed level of access. Access rights of users who have left are removed immediately. The building is adapted to meet the Scottish Government security requirements for the SCOTS network: ▪ access to the premises is controlled

	▪ all employees have met the requirements for receiving a Disclosure Scotland Certificate ▪ a cyber-resilience plan in place ▪ the SBC Clear Desk and Screen Policy details the procedures to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours ▪ the SBC Working from Home policy 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 details issues that must be considered to ensure that any SBC information worked on out of the office and shared off network is kept confidential and protected from loss of unauthorised access and exploitation ▪ a data security checklist is available for use in conjunction with the out of office security guidance Legislation will be met and the rights of data subjects protected. We must ensure that all contractors, or other trusted third parties who have access to personal data held or processed for or on behalf of SBC are aware of their duties and responsibilities under the DP Legislation
Protocol for security incidents	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Information Commissioner's office broadly defines a personal data breach as '… a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals' We must ensure we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the ICO and the affected individuals. We need a strategy for dealing with the breach, including: ▪ a recovery plan, including damage limitation ▪ assessing the likely risks to individuals as a result of the breach ▪ informing the appropriate people and organisations that the breach has occurred ▪ and reviewing our response and updating our information security All staff have a responsibility for reporting information security incidents, including any breaches of confidentiality. Staff must escalate security incidents to the Commissioner immediately to determine whether a personal data breach

	has occurred. On becoming aware of a security incident it is essential that it is managed effectively. The Commissioner will coordinate and ensure all the appropriate investigation and reporting processes are undertaken, and will liaise with the DPO where appropriate In the event of an SBC information security breach and/or files being misplaced or stolen, it is important to deal with the breach effectively. The breach may arise from a theft, a deliberate attack on our systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure. We must respond to and manage the incident appropriately. The following actions should be taken: ▪ the staff member should report the loss to the Commissioner within 24 hours or as soon as is practicably possible thereafter ▪ the Commissioner or in their absence, the relevant manager, should record the breach in a central database and is responsible for recording all the actions taken by the SBC to investigate and conclude the matter ▪ Data Protection legislation places a duty on the SBC to report certain types of personal data breach to the ICO. We must do this within 72 hours of becoming aware of the breach, where feasible ▪ if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay ▪ we must also keep a record of any personal data breaches, regardless of whether we are required to notify Important guidance on data security breach management and reporting breaches is available on the ICO website
Business continuity	We must have the ability to restore the availability and access to personal data in the event of a physical or technical incident in a 'timely manner'. See the SBC Business Continuity Plan

Data recording and storage

Accuracy	Data on any individual will be held in as few places as necessary, and all staff will be discouraged from establishing unnecessary additional data sets
Storage	Physical files are securely locked away within the office until destroyed. All work is stored on eRDM
Retention periods	SBC retention periods are set out in the Retention and Disposal Policy. We will keep some forms of information for longer than others. All staff are responsible for ensuring that information is not kept for longer than necessary

Archiving	The procedure for archiving and destroying data is set out in the Retention and Disposal Policy and supporting guidance and is managed by the Corporate Services Manager

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Annex 3

Protecting personal data

Tips for SBC staff on how to protect the personal data they hold:

- be aware that you can be prosecuted if you deliberately give out personal details without permission
- be wary of people who may try and trick you into giving out personal details; especially be aware of media requests
- do not open spam, not even to ask for no more mailings. Delete the email
- carry out any appropriate identity checks before giving out personal details when dealing with complaints;
    - must be satisfied that you are speaking to the complainant (or authorised person) before sharing any information
    - you can also ask for other details if in any doubt (address, email, phone etc.)
    - if still unsure, a good way is to call back on the number we hold
    - staff directly involved will usually have a relationship with the complainant and should really be the only people that need to share detailed information about a complaint
- carry out appropriate checks (of the information and recipient details) before sharing any information, by email, telephone or hardcopy
- only include necessary information when sharing (for example in emails, including internal emails) and anonymise / pseudonymise information as much as possible. Reference numbers should be sufficient in many cases
- consider whether the content of emails should be encrypted or password protected
- if sending a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending
- check you selected the correct email address before you press send. Consider copy and paste to reduce risk of incorrect address being typed, or incorrect autofill occurring
- be careful when using group email addresses
- make sure you use bcc if you do not want to reveal recipients in emails
- consider asking email recipients to acknowledge receipt of emails
- do not send offensive emails about other people, their private lives or anything else that could bring the SBC into disrepute
- consider whether it is appropriate to leave a message on an answering machine, and if you do minimise the personal data you include
- encrypt any personal information held electronically if it will cause damage or distress if it is lost or stolen
- all electronic devices leaving the office that contain confidential and personal data should be encrypted/password protected (with passwords held separately), especially where they contain sensitive information about individuals
- use strong passwords (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols
- do not share passwords
- dispose of all confidential paper waste in the bins provided (within SPSO office)

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

The above should be read in conjunction with SBC Records Management and Security Guidance: sharing information off network and out-of-office. Please also refer to the SBC Clear Desk and Screen Policy.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Annex 4

Subject Access Requests

Responsibility

Subject Access Requests are responded to by the IMSO/Business Support Officer and quality assured by the Corporate Services Manager.

Procedure for making request

Individuals have the right to access their personal data and the information set out below (subject to certain exemptions, for example, prejudice to our regulatory functions):

- the purpose and legal basis for the processing
- the categories of personal data concerned
- the recipients or categories of recipients to whom the personal data has been disclosed
- the period for which the personal data is to be preserved
- the existence of data subject's rights to rectification and erasure of personal data; the right to lodge a complaint with the Information Commissioner; and any information about the origin of the personal data.

Requests can be made verbally or in writing and do not have to refer to a subject access request, but it must be clear that the individual is asking for their own personal data. Requesters can, but do not have to, use the online contact form on our website to make a request, or email contact@biometricscommissioner.scot. For verbal requests, and those that are not clear, we should check with the requester that we have understood their request. We keep a record of all requests on an excel spreadsheet within Teams.

All staff are required to pass on anything which might be a subject access request to the IMSO/Business Support Officer without delay.

Provision for verifying identity

If we have doubts about the identity of the person making the request we can ask for more information. However, it is important that we only request information that is necessary to confirm who they are. The key to this is proportionality.

We need to let the individual know as soon as possible that we need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when we receive the additional information.

Third party requests

The Data Protection legislation does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If we think an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, we may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

There are cases where an individual does not have the mental capacity to manage their own affairs. Although there are no specific provisions in the UK GDPR, the Mental Capacity Act 2005 or in the Adults with Incapacity (Scotland) Act 2000 enabling a third party to exercise subject access rights on behalf of such an individual, it is reasonable to assume that an attorney with authority to manage the property and affairs of an individual will have the appropriate authority. The same applies to a person appointed to make decisions about such matters by, for example, the Sheriff Court.

Children

In Scotland, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown.

Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, we should consider whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights, then we should usually respond directly to the child. We may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

Charging

In most cases we cannot charge a fee to comply with a subject access request. However, where the request is manifestly unfounded or excessive we may charge a 'reasonable' fee for the administrative costs of complying with the request.

We can also charge a reasonable fee if an individual requests further copies of their data following a request. We must base the fee on the administrative costs of providing further copies.

Procedure for granting access

The SBC has one month to respond to an access request. Requests should be passed to the Business Support Officer straight away to log onto the excel spreadsheet, acknowledge, gather information, consult with relevant parties and respond. If staff respond directly to requests, they should consult the Business Support Officer in the first instance. Hard copy responses can be issued by secure courier.

If an individual makes a request electronically, we should provide the information in a commonly used electronic format, unless the individual requests otherwise. We can use encrypted email.

It is not acceptable to amend or delete the data if we would not otherwise have done so. Under the DPA, it is an offence to make any amendment with the intention of preventing its disclosure.
If we process a large amount of information about an individual we can ask them for more information to clarify their request. We should only ask for information that we reasonably need to find the personal data covered by the request.

We need to let the individual know as soon as possible that we need more information from them before responding to their request. The period for responding to the request begins when we receive the additional information. However, if an individual refuses to provide any additional information, we must still endeavour to comply with their request i.e. by making reasonable searches for the information covered by the request.

Further detailed guidance on subject access requests is on the ICO website.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Annex 5

Transparency

Commitment

Individuals have the right to be informed about the collection and use of their personal data, subject to exemptions. This is a key transparency requirement under the Data Protection legislation.

The SBC is committed to providing individuals with clear and concise information about what we do with their personal data. We will provide individuals with the following privacy information, the:

- name and contact details of our organisation
- name and contact details of our representative (if applicable)
- contact details of our Data Protection Officer (if applicable)
- purposes of the processing
- lawful basis for the processing
- legitimate interests for the processing (if applicable)
- categories of personal data obtained (if the personal data is not obtained from the individual it relates to)
- recipients or categories of recipients of the personal data
- details of transfers of the personal data to any third countries or international organisations (if applicable)
- retention periods for the personal data
- rights available to individuals in respect of the processing
- right to withdraw consent (if applicable)
- right to lodge a complaint with a supervisory authority
- source of the personal data (if the personal data is not obtained from the individual it relates to)
- details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to)
- details of the existence of automated decision-making, including profiling (if applicable)

Getting the right to be informed correctly can help the SBC to comply with other aspects of the Data Protection legislation and build trust with people, but getting it wrong can leave the SBC open to fines and lead to reputational damage.

Procedure

When we collect personal data from the individual it relates to, we must provide them with privacy information at the time we obtain their data.

When we obtain personal data from a source other than the individual it relates to, we need to provide the individual with privacy information:

- within a reasonable period of obtaining the personal data and no later than one month
- if we use data to communicate with the individual at the latest, when the first communication takes place or

- if we envisage disclosure to someone else, at the latest, when you disclose the data.

We must actively provide this information to individuals in a way that is easy to access, read and understand. We can meet this requirement in some cases by putting the information on our website, but we must make individuals aware of it and give them an easy way to access it.

When collecting personal data from individuals, we do not need to provide them with any information that they already have. When obtaining personal data from other sources, we do not need to provide individuals with privacy information if:

- the individual already has the information
- providing the information to the individual would be impossible
- providing the information to the individual would involve a disproportionate effort
- providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing
- we are required by law to obtain or disclose the personal data or
- we are subject to an obligation of professional secrecy regulated by law that covers the personal data.

We must regularly review and where necessary, update our privacy information. We must bring any new uses of an individual's personal data to their attention before we start the processing.

Data subjects will generally be informed in the following ways:

- Staff: all staff updates; website; orally
- Complainants/applicants: on the website; statements within communications; orally.

Responsibility
All staff have responsibility for ensuring privacy information is provided to data subjects.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Data Protection Impact Assessments

Our policy
Our Data Protection policy explains that we must carry out DPIAs in some circumstances and that it is good practice to do so whenever we are making changes to the way we process data. The policy can be found here.

Do we need a DPIA?
If your project / new process / process change:

- could change how we use/access/store/move personal data
- would lead to us contacting people in a new way
- would lead to people or organisations sharing information with us in a new way and/or
- requires you to obtain new personal data or to process personal data we hold as part of the project/process.

You should consider conducting a DPIA.

We may also consider carrying out a DPIA:

- following a data incident or near-miss
- when we identify or became aware of a risk and
- whenever we consider it is appropriate to review our existing processes.

Once complete, the DPIA should be sent to the DPO who will comment.

The comments will then be discussed and reviewed by the SBC team at the next Monthly Management Team meeting for a final decision.

Once approved the final documentation should be stored in the DPIA folder (see below for additional notes on version control.

Conducting a DPIA

Drafting a DPIA
The first part of the process is evidence gathering and you should consider at an early stage whether you need to consult stakeholders or not. It will not always be necessary to do so and the critical factors are likely to be:

- impact, is it likely to have significant impact
- scope, how many people or other processes would it impact
- whether there are options (if there is a statutory requirement we could consult on implementation but not on the requirement); and
- proportionality (a minor change may require a DPIA but may not require a full consultation).

The DPIA form will guide you through the questions and includes reference to some of the legal tests. There is also significant additional advice available on the ICO website and the DPO can provide ad-hoc support.

Obtaining approval
Generally, a DPIA will need to be approved before you start the project or make any changes to our systems/methods/processing of persona data.

The process for approval is:

- draft DPIA is shared with DPO for comments
- DPIA with DPO comments is shared with the SBC team for sign off.

DPIAs should be signed off at Monthly Management Team meetings. They will be reported in the Data Protection paper at quarterly Governance meetings.

Once signed off a copy of the DPIA should be stored in the DPIA folder.

Changes may also need to be made to the assessment as the project progresses. A working or live DPIA should be kept in the project folder to allow for this. Minor changes can be made by the project lead and approved retrospectively through the end of project formal DPIA sign-off process. Major changes will need to go through the approval process above.

Concluding the process
Once the project is complete. You should review and finalise the working/live DPIA noting any minor changes that occurred during the process.

The final DPIA should go through the same process as above. It is the project manager's (or owner's) responsibility to ensure that the final DPIA at the end of the project to save the document.

Privacy notices and Asset registers
We need to ensure our privacy notice and asset registers are up to date. If the DPIA identifies that these may need changed that should be highlighted to the Corporate Services Manager as soon as possible and before any new personal data is obtained or changes made to how we process data.

Version control
It is important that we keep an auditable track of the changes and, in particular of DPO comments. Version control should be used in the following way:

- first draft should be saved as 0.1
- minor changes should be saved as 0.2 etc.
- documents which have the Commissioner's approval or where the DPO has commented should be saved as major versions as 1.0

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Protocol for Data Security Incidents

Personal data breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. The Information Commissioner's office (ICO) broadly defines a personal data breach as '… a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the personal data or passes it on without proper authorisation; or if the personal data is made unavailable and this unavailability has a significant negative effect on individuals'.

Breach management

We must ensure we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the ICO and the affected individuals. We need a strategy for dealing with the breach, including:

- a recovery plan, including damage limitation
- assessing the likely risks to individuals as a result of the breach
- informing the appropriate people and organisations that the breach has occurred and
- reviewing our response and updating our information security.

All staff have a responsibility for reporting personal data security incidents, including any breaches of confidentiality. Staff must escalate incidents to the Commissioner immediately to determine whether a personal data breach has occurred. On becoming aware of a data security incident it is essential that it is managed effectively. The Commissioner will coordinate and ensure all the appropriate investigation and reporting processes are undertaken, and will liaise with the Data Protection Officer (DPO) as appropriate.

Process

In the event of a personal data breach it is important to deal with the breach effectively. The breach may arise from a theft, a deliberate attack on our systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure. We must respond to and manage the incident appropriately. The following actions must be taken:

- the staff member should report the incident to the Commissioner within 24 hours or as soon as is practicably possible thereafter by filling out a copy of the incident log with the available details
- the Commissioner or, in their absence, the relevant manager should record the incident in Teams and is responsible for updating the incident log and recording all the actions taken to investigate and conclude the matter
- the Commissioner should be informed as soon as possible of the incident and the action being taken, and must approve any decision to notify with the ICO
- the DPO should be informed as soon as possible of the incident and the action being taken, and should provide advice on actions.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Data Protection legislation places a duty on the SBC to report certain types of personal data breach to the ICO. Not all breaches need to be reported. If there is a likely risk to the rights and freedoms of individuals we must report to the ICO. We must do this within 72 hours of becoming aware of the breach, where feasible. The ICO website has information about reporting a breach here. This can be done by telephone or online. There is also a self-assessment tool to help determine if we need to report a breach. If we are unsure, we should call them for advice. Our registration number and date of registration ZB298978 (10 February 2022).

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay advising steps we are taking to mitigate effects and advice on protecting themselves and who to contact if they have concerns. We must keep a record of any personal data breaches, regardless of whether we are required to notify.

Breach examples

Some examples of incidents are where personal data has been disclosed in error by mail / email; where a file / mail / electronic device goes missing or is stolen; unauthorised access or alteration; or loss of availability of personal data. Some examples of personal data that could trigger a personal data security incident are data held on complaints and/or reviews.

Personal data breaches must be contained and data recovered as quickly as possible. Below are some of the recovery steps that will need to be taken in specific instances.

Personal data disclosed in error – the personal data should be retrieved as soon as possible and confirmation of deletion sought for any electronic data, as well as confirmation the information has/will not be further shared. (If the initial error was caused by use of cc instead of bcc in an email, take care to bcc recipients to advise of the error, apologise and advise on what steps those affected can take to mitigate further risks to themselves).

Missing mail – the person the mail is meant for (and where appropriate the person that logged the mail) must confirm searches in the first instance, before their entire team is asked to stop what they are doing to search, and then the whole office must search.

Theft – notify the police immediately, making sure you get an incident number and the name of the officer you spoke to.

Further guidance

Important guidance on personal data breach management and reporting breaches is available on the ICO website here.