



Scottish Biometrics
Commissioner
Coimiseanair
Biometrics na h-Alba

THE SCOTTISH BIOMETRICS COMMISSIONER

SCHEME OF GOVERNANCE AND RISK HANDBOOK

Version 2 May 2023



Safeguarding our biometric future



Document Control:

Title	Scheme of Governance and Risk Management Handbook
Prepared by	Cheryl Glen
Reviewed by	Dr Brian Plastow
Version	Version 2
Amendments	<ul style="list-style-type: none">Amended text throughout the document to better reflect current working practices including in particular Governance and Internal Control and the Scheme of Delegation
Date	May 2023



Contents

Governance and Internal Control

- Introduction
- Scottish Biometrics Commissioner (SBC) General Functions
- The Scottish Biometrics Commissioner
- Accountable Officer
- Audit
- Complaints
- Information Requests
- Subject Access and Data Protection
- Amendment to Governance Arrangements
- Scheme of Internal Control – Overview
- Monitoring Effectiveness
- Management Team and Leadership
- Governance Meetings

Scheme of Delegation

Code of Professional Conduct

- Introduction
- Guidance on the Code of Professional Conduct
- Compliance
- General Conduct
- Gifts and Hospitality
- Confidential Requirements
- Use of the SBC Office Facilities and ICT Equipment
- Appointment to Partner Organisations
- Contact with the Media
- Reporting of Improper Behaviour (Whistleblowing)
- Bribery and Fraud
- Corporate / SBC Policies and Procedures
- Equality and Fairness
- Registration of Interests
- Annex 1: Key principles of the Code of Conduct
- Annex 2: Definitions



Whistleblowing Policy

- Introduction
- Reporting a Concern – Internal Disclosures
- Investigating a Whistleblowing Disclosure
- Reporting a Concern – Regulatory Disclosures
- Protection after Making a Disclosure
- Independent Advice
- Annex 1: Public Concern at Work – Contact Details

Anti-Fraud Policy

- Introduction
- Prevention of Fraud
- Examples of Concerns
- Responsibilities
- Protection from Detrimental Treatment
- Internal Audit

Risk Management Policy

- Introduction
- Key Points
- Background
- Risk Management and Risk Registers
- Strategic Risk Register
- Roles and Responsibilities
- Risk Evaluation



Governance and Internal Control

Introduction

The Scottish Biometrics Commissioner (SBC) recognises that to deliver its strategic aims, objectives, and priorities successfully, it needs sound corporate governance and control mechanisms in place. Corporate governance is founded on laws, policies, processes, systems, and behaviours, and together they provide a system for the way in which an organisation is directed, administered, and controlled.

This handbook sets out the roles, responsibilities, and procedures for the effective and efficient conduct of the SBC business. It will be regularly reviewed so that it remains at the forefront of effective practice.

As a Scottish Public Authority, the Scottish Biometrics Commissioner is committed to governance excellence and to being accountable and transparent for its decisions and activities.¹

The aim of the handbook is to provide information about how the SBC operates, taking cognisance that the current make-up of the SBC is as a small Public Authority comprising of a single Commissioner and three members of staff. More about the Commissioner and their team can be found via the [website](#).

Scottish Biometrics Commissioner (SBC) General Functions

The general function of the SBC is to support and promote the adoption of lawful, effective, and ethical practices in relation to the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes by:

- The Police Service of Scotland ([Police Scotland](#))
- The Scottish Police Authority ([SPA](#))
- The Police Investigations and Review Commissioner ([PIRC](#))²

In furtherance of the Commissioner's general function, the SBC must prepare, and may from time-to-time revise, a Code of Practice on the acquisition, retention, use, and destruction of biometric data for criminal justice and police purposes.³ This Code must include provision about when biometric data must be destroyed in cases where a relevant enactment does not make such provision.⁴ Finally, the Code may make different provision for different purposes.

In exercising the general functions of the SBC, the Commissioner is required to:

¹ [Section 39](#) and [Schedule 2](#), Scottish Biometrics Commissioner Act 2020

² [Section 2](#), Scottish Biometrics Commissioner Act 2020

³ Sections 7 to 15, Scottish Biometrics Commissioner Act 2020

⁴ Relevant enactments – [Part 2 of the Criminal Procedure \(Scotland\) Act 1995](#); [Section 56 of the Criminal Justice \(Scotland\) Act 2003](#); [Chapter 4 of Part 4 of the Age of Criminal Responsibility \(Scotland\) Act 2019](#)



- Keep under review the law, policy, and practice relating to the acquisition, retention, use, and destruction of biometric data by or on behalf of those persons to whom the SBC functions extend
- Promote public awareness and understanding of the powers and duties those persons have in relation to the acquisition, retention, use, and destruction of biometric data, how those powers and duties are exercised, and how the exercise of those powers and duties can be monitored and challenged
- Promote and monitor the impact of the Code of Practice

Any function of the Commissioner may be exercised by a member of SBC staff authorised by the Commissioner, and to the extent authorised as set out in the [Scheme of Delegation](#).

The Commissioner may, with the consent of the Scottish Parliamentary Corporate Body (SPCB) as to the numbers, appoint staff. Staff appointed by the Commissioner are appointed on such terms and conditions as the Commissioner, with the approval of the SPCB determines.⁵

The Scottish Biometrics Commissioner

The Scottish Biometrics Commissioner is an independent public officeholder appointed by the late monarch Her Majesty the Queen on the nomination of the Scottish Parliament under the Scottish Biometrics Commissioner Act 2020.

The Commissioner is, in the performance of their duties, to be regarded as a juristic person distinct from the natural person holding office. The Commissioner is not, in the exercise of their general functions, subject to the direction or control of the Scottish Government or the Scottish Parliament.

The Commissioner's general function, as per [Section 2\(1\)](#) of the Act is to support and promote the adoption of lawful, effective and ethical practices in relation to the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes by the Police Service of Scotland, the Scottish Police Authority and the Police Investigations and Review Commissioner.

Accountable Officer

The Commissioner is the Accountable Officer (AO), designated by and answerable to the Scottish Parliamentary Corporate Body (SPCB). The AO's functions are to:

- Sign the Commissioner's accounts of expenditure and receipts
- Ensure the financial propriety and regularity of the SBC
- Ensure the Commissioner's resources are used economically, efficiently and effectively

In performing these functions, the Commissioner must:

- Keep proper accounts and accounting records
- Prepare in respect of each financial year a statement of accounts, and

⁵ [Schedule 1](#), Scottish Biometrics Commissioner Act 2020



- Send a copy of the statement to the Auditor General for Scotland for auditing.⁶

The Commissioner must comply with any direction which the Scottish Ministers give the Commissioner in relation to accounts, accounting records, and the annual statement of accounts.

Audit

External

The SBC's accounts will be audited each year by an external auditor appointed by the Auditor General for Scotland.

Internal

Internal audit services will be provided by an external organisation, appointed based on open tender.

Complaints

Customer Service Complaints

Complaints about the service provided will be handled in line with the Scottish Biometrics Commissioner [Complaints Handling Procedure](#).

Complaints about bodies within our jurisdiction not complying with our Code of Practice

Complaints can be made to the SBC about policing and criminal justice bodies within our jurisdiction not complying with the Code of Practice. Such complaints will be handled in line with the [Complaints Procedure](#) re Code of Practice⁷.

Information Requests

Requests for information under the [Freedom of Information \(Scotland\) Act 2002](#) (FOISA) will be handled in line with our policy Complying with Information Legislation (within our Information Governance Handbook). Complaints about requests for information under [FOISA](#), or [Environmental Information \(Scotland\) Regulations 2004](#) will be handled in line with the review and appeal routes as set out in the primary legislation.

⁶ [Section 31](#), Scottish Biometrics Commissioner Act 2020

⁷ [Section 15](#) of the Scottish Biometrics Commissioner Act



Subject Access and Data Protection

Subject Access Requests (SAR) and complaints about SAR and the processing of personal data will be handled in line with our policy Complying with Information Legislation (within our Information Governance Handbook). Complaints about Subject Access Requests under can be directed to the [ICO](#).

Amendment to Governance Arrangements

The governance arrangements and governance reporting arrangements can only be amended with the Commissioner’s approval. The Commissioner will inform the Advisory Audit Board (AAB) and the auditors of any amendments. The governance arrangements will be published as part of this handbook.

Scheme of Internal Control - Overview

The Scheme of Governance and Control (the Scheme) is a series of protocols and policies through which the Commissioner demonstrates they are meeting their responsibilities as the Commissioner and as the Accountable Officer. It also demonstrates the assurances they receive and the external scrutiny to which they are subject to.

SCHEME OF INTERNAL CONTROL

SCOTTISH BIOMETRIC COMMISSIONER

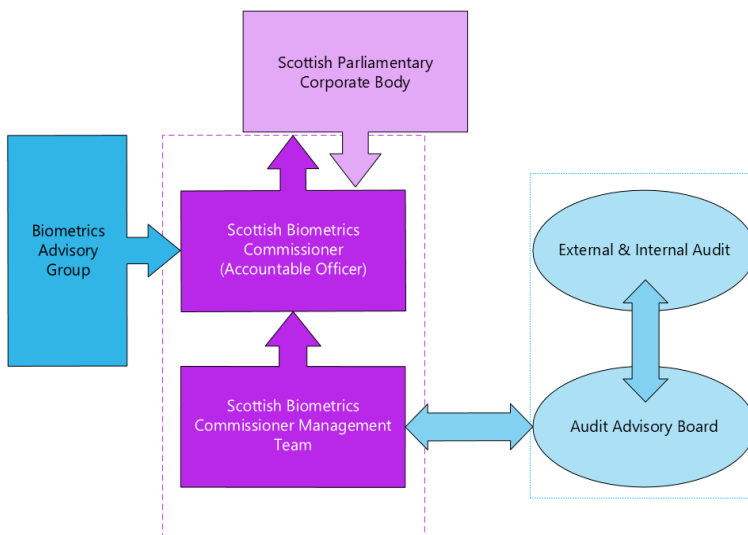


Figure 1: Scheme of Internal Control Schematic

The Scheme is supported by a [Risk Management Policy](#) and a [Strategic Risk Register](#). These define how the SBC monitors and manages risk in respect of:



- Achievement of and compliance with statutory obligations
- Achievement of strategic and operational objectives
- Establishment of and compliance with effective financial controls
- Achievement of and reporting on effective and efficient operational performance
- Effective asset management
- Ensuring the wellbeing of staff
- Developing and maintaining strategic relationships with partners and safeguarding the SBC's professional reputation

The key features of the Scheme are:

- The Commissioner is the Accountable Officer
- The Commissioner sets the strategic objectives and priorities supported by the SBC Management Team (Operations Manager, Corporate Services Manager and Business Support Officer)
- The Commissioner leads the SBC Management Team which has overall responsibility for the development of the SBC function
- The Operations Manager is responsible for external operations including maintaining and ensuring compliance with the statutory Code of Practice on biometric data by bodies to whom our functions extend, and for delivery of our external assurance function. The Operations Manager also has responsibility for investigating, monitoring and reporting on complaints made to us about potential non-compliance with our Code of Practice
- The Corporate Services Manager is responsible for internal corporate and business functions including investigating, monitoring, and reporting on customer service complaints. The Corporate Services Manager is also responsible for day-to-day financial and asset management and for the keeping of proper records and accounts. The Corporate Services Manager also has responsibility for our Records Management Plan (RMP) and ensuring compliance with Data Protection, Freedom of Information, and Subject Access obligations
- The Business Support Officer reports to the Corporate Services Manager and is responsible for all business support functions, including the maintenance of the public facing website and inbound and outbound correspondence. The Business Support Officer is also the designated Information Management Support Officer (IMSO) with responsibility to ensure that official records on the Electronic Records Document Management (ERDM) system are properly managed in line with statutory obligations
- All decisions by managers must be taken in line with the [Scheme of Delegation](#) and approved policies and procedures
- The Advisory Group on Biometric Data is established and maintained in accordance with the provisions of [Section 33 of the Scottish Biometrics Commissioner Act 2020](#). This is a biometrics



subject expert group with the function to give operational advice and information. It does not form part of the internal governance arrangements of the SBC

- External scrutiny and where appropriate advice, is provided by external auditors appointed by the Auditor General for Scotland; the Commissioner’s Advisory Audit Board; internal auditors appointed by the Commissioner, and on an ad hoc basis by the Scottish Parliamentary Corporate Body (SPCB) for those areas about which it can give direction or hold the Commissioner accountable.

Monitoring Effectiveness

The effectiveness of the Scheme and the robustness of the assurances it provides will be monitored and managed through:

- Periodic review of the definition, relevance, and accuracy of the measures, policies, and protocols in place
- Reports and Statements of Assurance from delegated officers
- Checking progress through reporting on achievement against strategic and business plans, individual projects, and ad hoc work programmes, and Statements of Assurance from external bodies such as the AAB, internal audit and external audit

Management Team and Leadership

The current staffing model for the SBC is four persons, comprising a management team of:

- The Commissioner
- The Operations Manager
- The Corporate Services Manager
- The Business Support Officer

This is necessitated by the constraints of budget as determined by the SPCB and is facilitated through mechanisms which enable the SBC to capitalise on shared-services and co-location (with physical and governance separation) with other Parliamentary Officeholders to achieve financial efficiencies and other economies of scale.

Accordingly, the leadership structure does not lend itself to ‘traditional’ leadership hierarchies of leaders, directors, managers, supervisors, and staff. Instead, and out of necessity the Commissioner and staff fulfil the strategic leadership, tactical management and operational delivery mechanisms and follow a very ‘flat’ structure as illustrated in Figure 1.

Purpose

The SBC Management Team is responsible for:



- Supporting the Commissioner in setting the strategic direction of the SBC
- Supporting the Commissioner in the exercise of their duties and responsibilities by developing and delivering the annual business plan and activities to deliver the [SBC four-year strategic plan](#)
- Participating in strategic, tactical, and operational leadership and delivery
- Ensuring that all legal obligations and duties are complied with
- Being accountable for the performance of the organisation
- Managing the financial position

Governance Meetings

To ensure the effectiveness of the Scheme of Governance and Control and the robustness of the assurances it provides, regular governance meetings will be held commensurate with the scale of the SBC staffing model. These may be summarised as:

Scottish Biometrics Commissioner – Governance and Control Meeting Schedule			
Meeting Level:	Meeting Type	Frequency	Attendees
Strategic (Gold)	Strategic Governance	Quarterly (Minutes & Actions taken and published)	Commissioner, SBC staff, SPCB Officeholder Services when required
Strategic (Gold)	Advisory Audit Board (AAB)	Six Monthly (Minutes & Actions taken and published)	Commissioner, SBC staff, AAB members
Tactical (Silver)	Management Team	Monthly (Minutes & Actions taken – and published)	Commissioner, SBC staff and invited representatives
Operational (Bronze)	Weekly team catch-up	Weekly No minutes required	Commissioner, SBC staff

Figure 2: SBC Governance and Control Meetings Schematic

The strategic, tactical, and operational governance meetings as illustrated in Figure 2 have the following purpose, frequency, agenda, and administrative arrangements:



Strategic Governance Meeting

PURPOSE	The quarterly governance meeting is to consider and sign-off corporate governance and strategic issues, and to provide the Commissioner with assurance that Scheme of Control protocols are being implemented effectively. Governance decisions may be taken between formal meetings but must be recorded and ratified at the next quarterly governance meeting	
FREQUENCY	Quarterly	
AGENDA	The agenda, venue and time of the meeting will be circulated no later than 5 working days before the meeting with any supporting papers	
ITEM	DESCRIPTION	LEAD
1	Minutes, actions and matters outstanding	Commissioner
2	Ratification of governance decisions taken between meetings	Commissioner
3	Strategic Plan	Commissioner
4	Strategic Risk Register	All
5	Business Plan <ul style="list-style-type: none"> ▪ KPI 1 – meet 4 x annually (PS, SPA, PIRC) ▪ KPI 2 – Advisory Group meets x 3 ▪ KPI 3 – one scale thematic review ▪ KPI 4 – publish 2 x newsletters ▪ KPI 5 – website footfall ▪ KPI 6 – compliance with CoP ▪ KPI 7 – Section 31 report ▪ KPI 7 – Section 32 report 	Commissioner Commissioner Operations Manager Business Support Officer Business Support Officer Operations Manager Corporate Services Manager Operations Manager
6	Stakeholder Engagement	Operations Manager
7	Budget & Finances	Corporate Services Manager
8	Audit(s)	Corporate Services Manager
9	Business Continuity	Corporate Services Manager
10	Complaints <ul style="list-style-type: none"> ▪ Code of Practice ▪ Customer Service 	Operations Manager Corporate Services Manager
11	FOI and SAR	Business Support Officer
12	ICT / Cyber-Resilience	Corporate Services Manager
13	Data Protection incl. Records Management	Corporate Services Manager
14	Wellbeing, Health & Safety, Employment matters	Commissioner
15	Any other business	All
ADMIN	The meeting will be chaired by the Commissioner, or in their absence the Corporate Services Manager. Except for annual leave or periods of absence, all managers will attend. The Business Support Officer will provide the secretariat function. Draft minutes will be circulated by the secretariat within seven working days of the meeting. They will be agreed at the next meeting and adopted as a permanent record before being published on	



the SBC website. Minutes will avoid the inclusion of personal data. If personal data is discussed at any meeting, then the minute will be appropriately redacted before publication in line with applicable exemptions under Freedom of Information legislation. Where any information is redacted, the reference to relevant sections of legislation should be included

Advisory Audit Board (AAB)

PURPOSE	The Advisory Audit Board independently monitors the management of risk and audit issues and gives advice to the Commissioner. This includes monitoring the integrity of SBC financial performance, statements, and budget submissions. The AAB review the effectiveness of SBC internal financial controls, other controls and performance and risk management systems. The AAB also review the SBC arrangements for employees to raise concerns in confidence, about possible wrongdoing in financial reporting or other matters. Ensuring that these arrangements allow proportionate and independent
FREQUENCY	Six monthly
MEMBERS	<u>Andrew Shaw (Chair); David Watt</u> ; the Scottish Biometrics Commissioner, Corporate Services Manager, Operations Manager; External Auditor, Internal Auditor, Business Support Officer
AGENDA	The agenda, venue and time of the meeting must be circulated no later than 5 working days before the meeting with any supporting papers. Standard agenda items will include:
ITEM	DESCRIPTION
1	Financial reporting
2	Internal controls, performance and risk management systems
3	Whistleblowing
4	Annual internal audit work plan
5	Reviewing and monitoring SBC responsiveness to findings or recommendations from internal audit
6	External audit
7	Reviewing and monitoring SBC responsiveness to findings or recommendations from external audit
8	Annual AAB Governance and Accountability report
ADMIN	The meeting will be chaired by Andrew Shaw. The Commissioner, Operations Manager, Corporate Services Manager and Business Support Officer will be in attendance – the latter providing the secretariat function. Other attendees such as the external or internal auditor will be determined by the Chair. They will be agreed at the next AAB meeting and adopted as a permanent record before being published on the SBC website



SBC Monthly Management Team Meeting

PURPOSE	The purpose of the monthly management team meeting is for the Commissioner and staff to share information and discuss tactical issues relating to the discharge of statutory obligations, corporate and operational performance, and progress with activity in support of the Strategic Plan	
FREQUENCY	Monthly	
AGENDA	The agenda, venue and time of the meeting must be circulated by the secretariat no later than 5 working days before the meeting with any supporting papers. Standard agenda items will include:	
ITEM	DESCRIPTION	LEAD
1	Welcome and apologies	Commissioner
2	Minutes, actions and matters outstanding	Commissioner
3	Operational Plan 1 – Thematic reports 2 – Laws of Retention 3 – Complaints 4 – Compliance Assessments 5 – Stakeholder Engagement 6 – Website incl. footfall 7 – Newsletters 8 – Research & Knowledge Exchange	Operations Manager Commissioner Operations Manager Commissioner Operations Manager Business Support Officer Business Support Officer Commissioner/Operations Manager
4	Policies & Procedures	Corporate Services Manager
5	Audit(s)	Corporate Services Manager
6	Data Protection	Corporate Services Manager / DPO
7	Cyber Security	Corporate Services Manager
8	Training	All
9	Annual Leave / Flexi Leave	All
ADMIN	<p>The meeting will be chaired by the Commissioner, or in their absence the Corporate Services Manager. Except for annual leave or periods of absence, all managers will attend. The Business Support Officer will provide the secretariat function</p> <p>Draft minutes will be circulated by the secretariat within seven working days of the meeting. They will be agreed at the next meeting and adopted as a permanent record before being published on the SBC website. Minutes will avoid the inclusion of personal data. If personal data is discussed at any meeting, then the minute will be appropriately redacted before publication in line with applicable exemptions under Freedom of Information legislation. Where any information is redacted, the reference to relevant sections of legislation should be included</p>	



Weekly Team Catch up meeting

Purpose	Frequency	Agenda
The purpose of the weekly team catch-up and briefing is to ensure that all members of staff are briefed on current operational and corporate issues and challenges and are aware of diary commitments for the week. This is necessary as the SBC will operate hybrid working arrangements where staff will work remotely from each other	Weekly on Mondays at 0930	The meeting will take the form of a collective informal briefing and team catch-up with reflections on the previous week and planned activities for the week ahead
Administrative arrangements The meeting will be chaired by the Commissioner, or in their absence the Operations Manager. The meeting will not require minutes		



Scheme of Delegation

I, **Brian Plastow, Scottish Biometrics Commissioner**, delegate to the under noted post-holders, the authority to exercise the following duties:

FINANCE	AUTHORISED SIGNATORY
Requests for goods and services, contracts and purchase orders up to and including £1000	<ol style="list-style-type: none"> 1. The Commissioner 2. Corporate Services Manager 3. Operations Manager
Requests for goods and services over £1000	<ul style="list-style-type: none"> ▪ The Commissioner
Invoice payment authorisation up to and including £1000	Originator of contract, countersigned by the Operations Manager
Invoice payment authorisation up to and including £2000	Originator of contract, countersigned by the Corporate Services Manager
Invoice payment authorisation over £2000	Originator of contract, countersigned by: <ul style="list-style-type: none"> ▪ The Commissioner
Approval of travel claims	Line manager of expense claim submitter
OFFICIAL DOCUMENTATION	AUTHORISED SIGNATORY
Contracts over £1000	<ul style="list-style-type: none"> ▪ The Commissioner
Purchase orders over £1000	<ul style="list-style-type: none"> ▪ The Commissioner ▪ Corporate Services Manager
Formal deeds and agreements	<ul style="list-style-type: none"> ▪ The Commissioner
Formal approval of SBC publications	<ul style="list-style-type: none"> ▪ The Commissioner
Formal approval of SBC press releases	<ul style="list-style-type: none"> ▪ The Commissioner
Freedom of Information requests	<ul style="list-style-type: none"> ▪ Business Support Officer ▪ Corporate Services Manager
Freedom of Information review requests	Either of the following who did not deal with the original request: <ul style="list-style-type: none"> ▪ The Commissioner



	<ul style="list-style-type: none"> Corporate Services Manager
PAYROLL	AUTHORISED SIGNATORY
Completed Monthly Payroll Submission and Summary	Corporate Services Manager
Salary Amendments (including advances, increases/decreases, new employee's annual salary)	The Commissioner
Overtime Claim Forms / payments of accrued holiday / TOIL / flexi upon leaving	The line manager or their line manager
Expense Claim Forms	<p>Amounts up to £500 - The line manager or their line manager</p> <p>Amounts over £1000 - The Commissioner</p>
Training courses	<p>One of the following:</p> <ul style="list-style-type: none"> The Commissioner Corporate Services Manager
Holiday Payments	<p>One of the following:</p> <ul style="list-style-type: none"> The Commissioner Corporate Services Manager
STAFFING	AUTHORISED SIGNATORY
Approving annual leave, overtime/TOIL and flexi-leave requests	The line manager or their line manager
Up to 10 consecutive days annual or other leave	The line manager or their line manager
Over 10 consecutive days annual or other leave	The Commissioner
Letters of appointment	The Commissioner and in their absence the Corporate Services Manager
Approval of training requests	<ul style="list-style-type: none"> The line manager or their line manager The Commissioner
Disciplinary matters	<ul style="list-style-type: none"> The line manager or their line manager The Commissioner
Staff objectives	The line manager or their line manager
Staff performance reviews	The line manager or their line manager
ABSENCE PROVISION	AUTHORISED SIGNATORY



In the event of the Commissioner’s prolonged absence	As per <u>Section 10(1)</u> of Schedule 1 to the SBC Act 2020 - in such circumstances the SPCB may appoint an individual to act as the Commissioner in their absence. To be eligible, the individual must be a member of the Commissioner’s staff, or someone who is not disqualified from holding the office of Commissioner under paragraph 3 of Schedule 1 i.e. an employee of Police Scotland, the SPA or PIRC
In the event of the Commissioner’s planned absence of two weeks or more	<ol style="list-style-type: none"> 1. Operations Manager 2. Corporate Services Manager
Where a member of staff is not contactable or unavailable, for example, on sick or prolonged leave, for a period beyond which a decision cannot be delayed, the authority is delegated as follows:	
The Commissioner	<ol style="list-style-type: none"> 1. Corporate Services Manager 2. Operations Manager
Operations Manager	<ul style="list-style-type: none"> ▪ Corporate Services Manager
Corporate Services Manager	<ol style="list-style-type: none"> 1. Operations Manager 2. Business Support Officer
COMPLAINTS	AUTHORISED SIGNATORY
Internal complaints	Should be directed to line manager or their line manager if the complaint is about them. If the complaint is about the Commissioner the SPCB will be notified so they can appoint at an external investigation officer
COMPLAINTS ABOUT THE FAILURE TO COMPLY WITH THE CODE OF PRACTICE	
A procedure for handling complaints about the failure to comply with the Code of Practice has been published on our website after being laid before the Scottish Parliament under <u>Section 13</u> of the SBC Act 2020	
Brian Plastow Scottish Biometrics Commissioner	May 2023



Code of Professional Conduct (incorporating the Register of Interests)

Introduction

The Scottish Biometrics Commissioner (SBC) is accountable to the Scottish Parliament for actions and decisions taken and has a duty to comply with any direction given to the Commissioner by the Scottish Parliamentary Corporate Body (SPCB) on certain matters.⁸

The [Ethical Standards in Public Life etc. \(Scotland\) Act 2000](#), does not apply to the Commissioner or SBC staff. However, as a listed Public Authority the SBC has adopted the general principles of the Act. Accordingly, the SBC will ensure that the conduct of staff is above reproach.

It is the responsibility of all SBC staff to be familiar and comply with the provisions of the SBC Code of Professional Conduct. The SBC Code of Professional Conduct applies to the Commissioner and all SBC staff.

Guidance on the Code of Professional Conduct (the Code)

The Commissioner and staff must observe the rules of conduct contained in this Code. It is an individual's responsibility to comply with and review regularly, and at least annually, personal circumstances particularly when any personal circumstances change. Staff must not at any time advocate or encourage any action contrary to the Code.

The Code has been developed in line with the key principles listed in [Annex 1](#) and provides additional information on how the principles should be interpreted and applied in practice. No Code of Professional Conduct can provide for all circumstances and if staff are uncertain about how the rules apply, they should seek advice from the Commissioner. If an allegation relating to professional conduct is made about the Commissioner, the allegation will be forwarded to the SPCB so that an external investigating officer may be appointed. The costs of such an independent investigation will be borne by the SBC.

Compliance

Breaches of the Code by staff may be considered a disciplinary matter under the SBC Disciplinary Procedures (within the Working for the SBC Handbook).

A breach of the Code by the Commissioner will be considered by the SPCB in terms of whether the circumstances also breach the Commissioners terms and conditions of appointment.

The Commissioner is responsible for monitoring and ensuring compliance with the Code and seeking advice and assurance from the Advisory Audit Board (AAB) as needed.

⁸ [Section 5](#) of the Scottish Biometrics Commissioner Act 2020



General Conduct

Staff must comply with any rules of the SBC regarding remuneration, allowances, and expenses. Staff must ensure any dealings with contractors or suppliers are fair and transparent and follow the SBC's Procurement Policy within the Finance Handbook.

Staff must respect and be courteous to all colleagues and behave in a manner which reflects the principles of the SBC's policies on Dignity at Work and Conduct & Behaviour (within the Working for the SBC acceptable).

Staff are expected when acting on behalf of the SBC to behave in a way that meets expectations and which reflects the organisation's values:

- Independent
- Transparent
- Proportionate
- Accountable

Staff must also be aware of [Section 19](#) of the SBC Act 2020, which creates a specific criminal offence for the Commissioner, SBC staff or an SBC agent to knowingly disclose confidential information unless it is otherwise authorised by the reasons outlined in Section 19(3).

Gifts and Hospitality

The SBC's policy is that staff should not canvass or accept gifts or hospitality for personal benefit because of their position. It is the individual's responsibility to ensure that their actions do not give rise to, or foster suspicion or perception that outside individuals or organisations have gained favour or advantage through the offer or acceptance of any gifts or hospitality. Further detailed information can be found within the Finance Handbook.

Staff must not accept any offer of a gift or hospitality from any individual or organisation which stands to gain or benefit from a decision the Commissioner's Office may be involved in determining; or from those seeking to do business with the SBC, which someone might reasonably consider could have a bearing on your judgement. When making a visit on behalf of the SBC as a rule, staff should ensure that the SBC pays for the costs of the visit unless funded or part-funded by the Parliament or Scottish Government.

Additionally, staff must not offer, promise, or give a gift, hospitality or other benefit to a third party which may be perceived as inducing that person or organisation to perform a relevant function or activity improperly.

Staff are responsible for their decisions connected with the offer or acceptance of gifts or hospitality and for avoiding the risk of damage to public confidence in the SBC. As a general guide, it is usually appropriate to refuse offers except:



- isolated gifts of a trivial character or inexpensive seasonal gifts such as a calendar or diary, or other simple items of office equipment of modest value
- normal hospitality associated with your duties, and which would reasonably be regarded as inappropriate to refuse, or
- gifts received on behalf of the SBC

Staff should also consider whether there may be any reasonable perception that any gift received by their spouse or partner, or by any company in which they have a controlling interest, or by a partnership of which they are involved, can or would influence their judgement. The term 'gift' includes benefits such as relief from indebtedness, loan concessions, or provision of services at a cost below that generally charged to members of the public.

Staff must not accept repeated hospitality from the same source. Staff must record details of any gifts and hospitality received with the Business Support Officer over the amount of £50. This record will be made available for public inspection.

Confidentiality Requirements

Section 19 of the Scottish Biometrics Commissioner Act 2020 makes it an offence for the Commissioner, a member of the Commissioner's staff, or an agent of the Commissioner to disclose confidential information except in accordance with the exercise of the Commissioner's functions under the Act or in accordance with the exceptions stated at Section 19(3).

Use of the SBC Office Facilities and ICT Equipment

Staff must not misuse facilities, equipment, stationery, telephony and services, or use them for party political or campaigning activities. Use of such equipment and services etc. must be in accordance with the IT Security (Shared Services Policy and the ICT Strategy (Shared Services) and rules on their usage.

Appointment to Partner Organisations

Staff may be appointed or nominated by the Commissioner as a member of another body or organisation. If so, staff are also bound by the rules of conduct of those organisations and should observe the rules of this Code in carrying out the duties of that body.

Contact with the Media

The Scottish Biometrics Commissioner will respond to media enquiries from journalists who are accredited and in possession of a UK Press Card as managed by the UK Press Card Authority. All such enquiries will be directed to the Commissioner. The Commissioner will seek to accommodate requests considered against the public interest and impact on the delivery of the SBC functions.



Reporting of Improper Behaviour (Whistleblowing)

Under the [Public Interest Disclosure Act 1998](#), if you see or witness or feel you have seen or witnessed or are being required to witness a colleague or manager of other person acting in a way which may be illegal, improper, unethical or in conflict with this Code of Professional Conduct, then please refer to the [Whistleblowing Policy](#) for advice and guidance.

Bribery and Fraud

Any activity or behaviour which is found to be bribery or fraud will not be tolerated. The SBC encourages a culture of integrity where bribery and fraud is unacceptable. Please see the [Anti-fraud Policy](#) for advice and guidance.

Corporate / SBC Policies and Procedures

Staff are expected to comply with all SBC and Shared Services policies and procedures at all times during employment. Staff must act in good faith at all times and ensure their conduct or professionalism is without question. All policies and procedures can be found on our website.

Equality and Fairness

Staff should be able to expect fair and reasonable treatment at work in line with the SBC's values and policies on equality, diversity and dignity at work (within the Working for the SBC handbook). The SBC views discrimination, harassment, victimisation and bullying at work as a serious matter. If staff feel they have been a victim of unfair treatment you should raise the matter with the Commissioner or HR.

Registration of Interests

Staff must declare and record any personal interest that might influence or be seen by others to influence their impartiality in arriving at a decision. Those who have business or personal relationships with, or friends/relatives employed by outside organisations bidding for SBC contracts must inform the Commissioner at the outset.

The following paragraphs set out the categories of interests, financial and otherwise, which staff must register. These are 'Registerable Interests' and staff must ensure that they are registered. The register is maintained by the Corporate Services Manager.

It is an individual's personal responsibility to comply with these regulations and they should be reviewed regularly, and at least once a year. [Annex 2](#) contains key definitions and explanatory notes to help staff decide what is required when registering their interests under any category. It is not necessary to register the interests of a spouse, civil partner or cohabitee.



Category one: Remuneration

You have a registerable interest where you receive remuneration by virtue of being:

- employed other than by the SBC
- self-employed
- the holder of an office
- the director of an undertaking
- a partner in a firm, or
- undertaking a trade, profession, or vocation, or any other work

If you do have other remunerable income from one or more of these categories the amount of remuneration does not require to be registered. If a position is not remunerated it does not need to be registered under this category. However, unremunerated directorships may need to be registered under category two 'Related Undertakings'.

If you receive any allowances in relation to membership of any organisation the fact that you receive such an allowance must be registered. When registering employment, you must give the name of the employer, the nature of its business and the nature of the post held in the organisation.

When registering self-employment, you must provide the name and give details of the nature of the business. When registering an interest in a partnership, you must give the name of the partnership and the nature of its business.

Where you otherwise undertake a trade, profession or vocation, or any other work, the detail to be given is the nature of the work and its regularity. For example, if you write for a newspaper you must give the name of the publication and the frequency of articles for which you are paid. When registering a directorship, it is necessary to provide the registered name of the undertaking in which the directorship is held and detail the nature of its business.

Registration of a pension is not required as this falls outside the scope of the category.

Category two: Related Undertakings

You must register any directorships held which are themselves not remunerated but where the company (or other undertaking) in question is a subsidiary of, or a parent of, a company (or other undertaking) in which you hold a remunerated directorship.

You must register the name of the subsidiary or parent company or other undertaking and the nature of its business, and its relationship to the company or other undertaking in which you are a director and from which you receive remuneration.

The situations to which the above paragraph apply are: (a) where you are a director of a board of an undertaking and receive remuneration declared under Category one, and (b) you are a director of a parent or subsidiary undertaking but do not receive remuneration in that capacity.



Category three: Contracts

You have a registerable interest where you (or a firm in which you are a partner, or an undertaking in which you are a director or in which you have shares of a value) have made a contract with the SBC:

- under which goods or services are to be provided, or works are to be executed, and
- which has not been fully discharged

In such circumstances, you must register a description of the contract, including its duration.

Category four: Houses, Land and Buildings

You have a registerable interest where you own or have any other right or interest in houses, land, and buildings in the United Kingdom, which may be significant to, of relevance to or bear upon the work and operation of the SBC.

The test to be applied when considering appropriateness of registration is to ask whether a member of the public acting reasonably might consider any interests in houses, land and buildings could potentially affect your responsibilities to the SBC and to the public or could influence your actions or decision-making. If in doubt, seek advice from the Commissioner.

You are required to give the address of the property, or otherwise give a description sufficient to identify it. **However, under no circumstance will the private address of the Commissioner or of SBC staff be disclosed to anyone other than the SBC, the SPSO or the Scottish Parliamentary Corporate Body.**

Category five: Interest in Shares and Securities

You have a registerable interest where you have an interest in shares which constitute a holding in a company or organisation which may be significant to, of relevance to, or bear upon the work and operation of the SBC and the nominal value of the shares is:

- greater than 1% of the issued share capital of the company or body, or
- greater than £25,000 (you are not required to register the value of such interests)

The test to be applied when considering appropriateness of registration is to ask whether a member of the public acting reasonably might consider any interests in shares and securities could potentially affect your responsibilities to the SBC and to the public or could influence your actions or decision-making. If in doubt, seek advice from the Commissioner.

Category six: Non-Financial Interests

You may also have a registerable interest if you have non-financial interests which may be significant to, of relevance to, or bear upon the work and operation of the SBC. It is important that relevant interests such as membership or holding office in other public bodies, clubs, societies, and organisations such as trades unions and voluntary organisations are registered and described.



The test to be applied when considering appropriateness of registration is to ask whether a member of the public acting reasonably might consider any non-financial interest could potentially affect your responsibilities to the SBC and to the public or could influence your actions or decision-making. If in doubt, seek advice from the Commissioner.

Declaration of Interests

The key principles of the Code of Professional Conduct, especially those in relation to integrity, honesty, and openness are given further practical effect by the requirement for you to declare certain interests in proceedings of the SBC. This ensures the transparency of your interests which might influence, or be thought to influence your actions.

Public bodies inevitably have dealings with a wide variety of organisations and individuals and this Code indicates the circumstances in which a business or personal interest must be declared. Public confidence in the SBC depends on it being clearly understood that actions and decisions are taken in the public interest and not for any other reason.

Interests which Require Declaration

Interests which require to be declared may be financial or non-financial. They may or may not be interests which are registerable under this Code. Most of the interests to be declared will be your personal interests but, on occasion you will have to consider whether the interests of other persons require you to make a declaration.

Interests of Other Persons

The Code requires only your interests to be registered. You should however consider whether you wish to declare a connection to the financial interests of your spouse, civil partner, or co-habitee which are known to you. You should ask yourself whether a member of the public acting reasonably would regard these interests as effectively the same as your interests in the sense of potential effect on your responsibilities within the SBC.

The interests known to you, both financial and non-financial, of relatives and close friends may have to be declared. The Code does not attempt the task of defining 'relative' or 'friend'. The key principle is the need for transparency about any interest which might (regardless of the precise description of relationship) be objectively regarded by a member of the public, acting reasonably, as potentially affecting your responsibilities within the SBC.

Making a Declaration

You must consider at the earliest stage possible whether you have an interest to declare in relation to any matter which is to be considered. You must declare the interest as soon as you realise it is necessary to do so.



Effect of Declaration

Declaring an interest, financial or otherwise, has the effect of prohibiting your involvement in the decision-making of the matter under consideration.



Annex 1: Key Principles of the Code of Conduct

Public Service

You have a duty to act in the interests of the public body of which you are a member and in accordance with the core tasks of that body.

Selflessness

You have a duty to take decisions solely in terms of public interest. You must not act to gain financial or other material benefit for yourself, family or friends.

Integrity

You must not place yourself under any financial or other, obligation to any individual or organisation that might reasonably be thought to influence you in the performance of your duties.

Objectivity

You must make decisions solely on merit when carrying out public business.

Accountability and Stewardship

You are accountable for your decisions and actions to the public. You have a duty to consider issues on their merits, taking account of the views of others and must ensure that the public body uses its resources prudently and in accordance with the law.

Openness

You have a duty to be as open as possible about your decisions and actions, giving reasons for your decisions and restricting information only when the wider public interest clearly demands.

Honesty

You have a duty to act honestly. You must declare any private interests relating to your public duties and take steps to resolve any conflicts arising in a way that protects the public interest.

Leadership

You have a duty to promote and support these principles by leadership and example, to maintain and strengthen the public's trust and confidence in the integrity of the public body and its members in conducting public business.

Respect

You must respect fellow members of your public body and employees of the body and the role they play, always treating them with courtesy.



Annex 2: Definitions

A person

Means a single individual or legal person and includes a group of companies.

Any person

Includes individuals, incorporated and unincorporated bodies, trade unions, charities and voluntary organisations.

Co-habitee

Includes a person, who is living with you in a relationship like that of a spouse.

Group of companies

Has the same meaning as 'group' in [Section 1261 of the Companies Act 2006](#). A group, within Section 1261 of the 2006 Act means:

'In relation to a body corporate, means the body corporate, any other body corporate which is its holding company or subsidiary and any other body corporate which is a subsidiary of that holding company'.

Parent Undertaking

Is an undertaking in relation to another undertaking a subsidiary undertaking if a) it holds a majority of the voting rights in the undertaking; or b) it is a member of the undertaking and has the right to appoint or remove a majority of its board of directors; or c) it has the right to exercise a dominant influence over the undertaking (i) by virtue of provisions contained in the undertaking's memorandum or articles or (ii) by virtue of a control contract; or d) it is a councillor of the undertaking and controls alone, pursuant to an agreement with other shareholders or councillors, a majority of the voting rights in the undertaking.

Public Authority

Means a body carrying out tasks or functions in the public interest, or in the exercise of official authority vested in it.

Related Undertaking

Is a parent or subsidiary company of a principal undertaking of which you are also a director. You will receive remuneration for the principal undertaking though you will not receive remuneration as director of the related undertaking.

Remuneration:

Includes any salary, wage, share of profits, fee, expenses, other monetary benefit, or benefit in kind. This would include for example, the provision of a company car or travelling expenses by an employer.

Spouse

Does not include a former spouse or a spouse who is living separately and apart from you.



Undertaking

a) a body corporate or partnership or b) an unincorporated association carrying on a trade or business, with or without a view to a profit.



Whistleblowing Policy

The term 'whistleblowing' is not legally defined. It is generally understood to mean drawing attention to alleged wrongdoing internally where there is a proper mechanism for doing so, or externally where such a mechanism is lacking.

Introduction

This policy sets out the Scottish Biometrics Commissioner's (SBC) approach to whistleblowing and provides guidance to staff about raising concerns. It is intended to encourage and enable staff to raise concerns within the SBC, rather than overlooking a problem or blowing the whistle outside. The policy takes account of the [Public Interest Disclosure Act 1998](#) (PIDA).

The SBC is committed to the highest standards of honesty, openness and accountability. As a part of this commitment the SBC encourages staff with concerns about any aspect of its work to come forward and express these concerns.

All whistleblowing disclosures are treated in confidence. The SBC will do all it can to protect the identity of a staff member who raises a concern and does not want their name to be made known. However, there may be situations where a matter cannot be investigated unless the identity of the staff member is known. The implications of making their identity known are discussed fully with the staff member beforehand and protective measures put in place, if required.

Reporting a Concern – Internal Disclosures

Staff members who have a concern; become aware of wrongdoing; or consider they have been asked to act in way that raises a fundamental issue of conscience for them should speak to their line manager or the Commissioner in confidence. Staff also have the option to raise concerns with HR.⁹

If it is inappropriate or difficult for the staff member to raise a concern with their line manager, or the concern is about the line manager, then the concern can be discussed with HR. If their line manager is the Commissioner then they should address their concern with the Scottish Parliamentary Corporate Body.

If the staff member does not consider that the response received from the line manager or HR is reasonable, then they may take their concern directly to the Commissioner. If the concern relates to the Commissioner, then the staff member may take the concern to the Scottish Parliamentary Corporate Body who will determine how to proceed.

The Commissioner must be told about the existence of any whistleblowing disclosures, protecting the identity of the whistle blower as far as possible. As soon as the initial facts are established, the person receiving the disclosure must give a written summary of the discussion to the Commissioner. Initial enquiries may be made to decide whether an investigation is appropriate. Some concerns may be resolved

⁹ SBC staff are employed under the same terms and conditions as SPSO staff and HR services are provided to the SBC by the SPSO.



by agreed action without the need for investigation. If urgent action is required, this may be taken before any investigation is conducted. The Commissioner makes the decision to initiate an investigation. The Commissioner will report all incidents of whistleblowing to the Advisory Audit Board for information and advice.

Investigating a Whistleblowing Disclosure

Unless the disclosure is about the Commissioner, the Commissioner will either investigate the disclosure or may delegate the role of Investigating Officer to an appropriate manager. If criminal activity is suspected, the Commissioner will contact Police Scotland to determine the nature and extent of any police involvement in the investigation.

The purpose of an investigation is to establish the relevant facts. An investigation takes place as sensitively and speedily as possible. It may not be possible to give precise timescales in an investigation, but time limits should be allocated for each stage of the procedure.

The outcome of an investigation is reported to the Commissioner who determines what action to take.

Reporting a Concern – Regulatory Disclosures

SBC staff are encouraged to raise concerns internally. However, there may be circumstances when a staff member has disclosed a concern internally but is not satisfied by either the response after investigation or the lack of response. In addition, there may be situations where the staff member is unable or afraid to talk to anyone internally because of the nature of the concern.

The [PIDA](#) sets out the circumstances in which it is appropriate to report concerns to an external body. It makes special provision for disclosure to 'prescribed persons' where a staff member reasonably believes the wrongdoing falls within their remit. These are known as regulatory disclosures.

Protection after Making a Disclosure

The [PIDA](#) states that a worker has the right not to be subjected to any detriment by any act, or any deliberate failure to act, by his/her employer on the ground that the worker has made a protected disclosure. The legislation does not introduce a general protection for whistle blowers that applies in all circumstances. It applies to workers who follow the procedures laid down in the legislation, as set out above in disclosing specific categories of wrongdoing.

A staff member would not qualify for protection if they were committing an offence by disclosing the information (for example, if disclosure was prohibited under the Official Secrets Act 1989). Confidentiality clauses such as gagging clauses in employment contracts and severance agreements that conflict with the protection provided by the [PIDA](#) are not legally binding.



Independent Advice

A staff member who is unsure whether to use the Whistleblowing Policy, or would like independent advice at any stage is encouraged to seek legal advice, contact their trade union for advice or contact an advice agency such as the independent charity Public Concern at Work (see [Annex 1](#) for details).

A qualifying disclosure is protected if it is made to a legal adviser while obtaining legal advice. Staff members who seek other advice should bear in mind the distinction between seeking information about the provisions of the [PIDA](#) and the requirements attached to making a protected disclosure.



Annex 1: Public Concern at Work – Contact Details

Public Concern at Work is the leading authority on public interest whistleblowing. Its charitable objectives are to promote compliance with the law and good practice in organisations across all sectors. In practical terms, it focuses on the responsibility of workers to raise concerns about wrongdoing and the responsibility of those in charge to investigate and remedy such issues. It provides free advice and assistance to individuals who are concerned about apparent danger or wrongdoing in the workplace.

UK Office

Public Concern at Work
3rd Floor, Bank Chambers
6 - 10 Borough High Street
London SE1 9QQ

Telephone: 020 7404 6609 (general enquiries and helpline)

Fax: 020 7404 6576

Email: whistle@pcaw.co.uk (UK enquiries); helpline@pcaw.co.uk (UK helpline); services@pcaw.co.uk (UK services)

Website: www.whistleblowing.org.uk

Hours: The UK office is open and the helpline is staffed from 09:00 to 18:00 Monday to Friday. There is an answering machine out-of-hours

Scottish Office

Public Concern at Work
The Nerve Centre
80 Johnstone Avenue
Hillington Business Park
Glasgow
G52 4NZ

Telephone: 0141 883 6761 (general)

Email: ht@pcaw.co.uk

The Office is staffed weekday mornings and helpline calls are rerouted to the UK lawyers based in London.



Anti-Fraud Policy

Introduction

In Scotland, the term 'fraud' refers to the **deliberate use of deception or dishonesty** to disadvantage or cause loss to another person or party. Criminal fraud in Scotland is dealt with under common law (unwritten law based on custom or previous court decisions). Fraud can comprise of:

- Common law fraud
- Forgery and uttering
- Embezzlement
- Statutory frauds

The Scottish Biometrics Commissioner (SBC) is a Public Authority charged with independent oversight of how highly sensitive biometric data is managed within the policing and justice sector in Scotland. The SBC requires absolute honesty and integrity from its staff. Our anti-fraud policy is essential to ensure the highest standards of propriety and integrity and should be read in conjunction with the following policies:

- [Scheme of Governance and Control](#)
- [Scheme of Delegation](#)
- [Whistleblowing Procedure](#)
- Gifts and Hospitality Procedure (within Finance Handbook)
- Grievance Procedure (within Working for the SBC Handbook)
- Travel and Subsistence Policy (within Finance Handbook)
- Disciplinary Procedure (within Working for the SBC Handbook)
- Conduct and Behaviour Procedure (within Working for the SBC Handbook)

This policy is concerned with occupational fraud, i.e. fraud committed by SBC staff or contractors in the course of their work. Occupational fraud and abuses fall into four main categories:

1. Theft, and the misappropriation or misuse of assets for personal benefit
2. Bribery and corruption
3. False accounting and/or making fraudulent statements with a view to personal gain or gain for another (for example falsely claiming overtime, expenses, or subsistence)
4. Externally perpetuated fraud against an organisation

All policies and practices adopted by the SBC to safeguard the organisation against fraud are in line with the fraud section of the [Scottish Public Finance Manual](#) (SPFM).

Prevention of Fraud

The Commissioner is committed to preventing fraud and corruption from occurring, to having appropriate systems of detection and correction in place and to maintaining an anti-fraud culture. To achieve this, the SBC will comply with the requirements of Government Accounting to:



- Assess the organisation's overall vulnerability to fraud and the specific areas which are most vulnerable
- Develop and maintain effective controls to prevent fraud
- Ensure that if fraud occurs a vigorous and prompt investigation will take place
- Take appropriate disciplinary and legal action, where justified
- Review systems and procedures to prevent similar frauds
- Investigate whether there has been a failure in supervision and take appropriate disciplinary action where supervisory failures are identified
- Record and report all discovered cases of fraud

The Commissioner will not tolerate fraud, impropriety, or dishonesty. Any such instances will be investigated by SBC staff or where appropriate an external organisation. If criminality is suspected, the circumstances will be reported by the Commissioner to Police Scotland.

The SBC will cooperate fully with any external investigating body and will always seek to recover any public funds misappropriated through fraud.

The SBC will maintain a Fraud Register in which it will log details of all allegations of fraud and the outcome and conclusions from investigation.

Examples of Concerns

Concerns which should be reported include, but are not limited to, staff committing, attempting to commit, or being an accessory to:

- Any dishonest or fraudulent act
- Forgery or alteration of documents or accounts with intent to deceive
- Misappropriation of funds, supplies or other assets
- Impropriety in the handling or reporting of money or financial transactions
- Profiting from an official position
- Disclosure of official activities or information for advantage
- Accepting or seeking value from third parties by virtue of official position or duties
- Theft or criminal misuse of property, facilities, or services

External organisations' actions which should be reported include but are not limited to:

- The offering of a bribe or inducement by a supplier
- Fraudulent invoices from a supplier
- Corruption or deception on the part of a supplier



Responsibilities

The maintenance of an anti-fraud culture underpins all work to prevent and counter fraud. All SBC staff should understand the risk of fraud and the negative impact on the reputation of the SBC. Responsibilities are as follows:

Commissioner

- Maintain adequate systems of control to mitigate risk relating to fraud occurring, going undetected, and not being properly challenged
- Appoint an appropriate independent person to investigate allegations of fraud and approve investigative strategy
- Report all incidents of fraud to the Advisory Audit Board

Corporate Services Manager

- Actively manage risk relating to fraud in line with the [Risk Management Policy](#) and enforce the SBC Anti-Fraud policy
- Appoint an independent investigator approved by the Scottish Parliamentary Corporate Body if the allegation is about the Commissioner
- Communicate this policy and any amendments to all staff

Other Managers

- Provide assurance to the Commissioner of the adequacy of systems to manage the risk related to fraud
- Report any instances of suspected fraud in line with the governance arrangements

Protection from Detrimental Treatment

The [Public Interest Disclosure Act 1998](#) gives some protection to individuals from detrimental treatment (victimisation or dismissal) for raising serious concerns about matters in the public interest. This could include criminal activity such as fraud. For further information see the SBC [Whistleblowing Policy](#).

Internal Audit

Internal audit is an independent appraisal function established by the management of an organisation for the review of the internal control system as a service to the organisation. It objectively examines, evaluates and reports on the adequacy of internal control as a contribution to the proper, economic, efficient and effective use of resources.

Internal auditors will be appointed by the SBC to review and test the internal controls of key financial and non-financial systems. The key factors for successful internal audit are:



- Setting clear and properly focussed objectives for internal audit
- Maintaining internal audit independence
- Planning and controlling the work of internal audit
- Resourcing the internal audit work programme
- Having effective reporting and follow-up arrangements
- Holding internal audit to account for its performance

The modest scale of the SBC suggests the need for a proportionate approach to internal audit having regard to the limited finances and resources of the organisation. As the SBC benefits from a shared-service arrangement with the SPSO around certain corporate functions we will appoint different internal auditors from the SPSO, so that the propriety of the shared arrangements can be independently assessed and validated.

The nature of the function of the SBC requires reliable and robust internal audit. This will be implemented and managed by the Corporate Services Manager, reporting to the Commissioner and the SBC Management Team.



Risk Management Policy

Introduction

This policy sets out the steps that need to be followed to identify and manage business risk. It also outlines procedures to support staff to navigate the system of incident reporting, incident investigation and associated learning.

Key Points

- Risk management is part of business planning, strategic and operational decision making and business continuity
- To manage risk effectively, the Scottish Biometric Commissioner (SBC) needs to define their risk appetite, to ensure resources are prioritised in the right areas and to encourage management to take appropriate risks where it will generate the highest value
- A risk needs to threaten the achievement of the SBC's strategic and business aims to be included in the risk register
- One of the key elements of internal control will be ensuring that the SBC Management Team consider risk when making decisions
- The risk register should only contain risks that the SBC is able to manage and control or to minimise the impact on the SBC should the risks materialise
- The SBC Management Team should ensure that risk assessment is embedded into corporate and performance management, business planning and financial reporting processes and not carried out as an isolated exercise
- It is recognised good practice to record and report data, security, and health and safety incidents which occur to ensure that learning and improvement takes place.

Background

This policy outlines the steps that need to be followed to identify and manage key risks to the achievement of the SBC's business objectives in line with good practice. Risk management should therefore be closely linked to the business planning process. There should also be a link between risk management, business planning and plans for business continuity.

Risk Management and Risk Registers

Strategic risks will be set at the start of the Strategic Plan running for the life cycle of the plan, they will be reviewed at the start of each financial year, as part of the business planning process which involves all staff and amended as necessary. The strategic risk register is the mechanism by which links are made between strategic objectives and operational delivery and performance of services.



Strategic Risk Register

The strategic risk register sets out the strategic risks that impact on several areas of business and relate specifically to the Strategic Plan. The four-year Strategic Plan will be signed off by the Commissioner, with advice from the Advisory Audit Board. The number of strategic risks on the register should be proportionate to the number of strategic objectives.

The risk register will be reviewed and updated annually. Changes must be agreed by the Commissioner recorded as part of Governance meetings.

Roles and Responsibilities

A process of corporate evaluation of the known risks, the SBC Management Team should aim to arrive at an overall list (grouped as appropriate) of the key risks confronting the SBC.

As part of their responsibility for internal control and as part of an effective business planning process the SBC Management Team should meet at least quarterly to review the key business risks associated with achievement of the SBC's strategic objectives. It is for the SBC Management Team to judge the impact of all potential key risks (not only financial risks) and to consider how they should be managed.

The five main objectives of the quarterly review of the risk register(s) should be to:

1. Discuss, evaluate and agree the list of business risks which might affect the ability to deliver objectives and targets
2. Assess existing controls (the measures in place to reduce or limit risk)
3. Determine the appropriate response to each risk
4. Allocate responsibility for managing each risk, and
5. Agree future review procedures

Risk Evaluation

Taking each risk in turn, the SBC Management Team will discuss and rate the likelihood of each risk occurring and its overall impact. This is done by assessing and awarding a numerical value where the lowest risk = 1 and the highest = 5. By multiplying the likelihood by impact scores and overall inherent risk rating is determined using the following scale.

Score	Grade
1-5	VERY LOW risk
6-10	LOW risk
12-15	MODERATE risk
16-20	HIGH risk
25	VERY HIGH risk