251001 (202) FOI Fraud Policy

From: Freedom of Information
To: [redacted]
Cc: Freedom of Information
Subject: Freedom of Information Request
Date: 01 October 2025 08:58:00
Attachments: [redacted]

Dear [redacted]

Thank you for your Freedom of Information request of 9 September 2025. We are responding to you under the Freedom of Information (Scotland) Act 2002 [FOISA].

FOI REQUEST (9 September 2025)
Could you please send me a copy of the SOSE policies and processes for fraud investigations.

RESPONSE
SOSE's Counter Fraud Policy is attached. The policy is due for a review following changes in our organisational structure and Director job titles. The Director of Finance and Corporate Resources job title was recently changed to Director of Business Enablement which is the role of [redacted]. As outlined in the policy (Appendix 1 - paras 1.11-1.14), suspected instances or allegations of fraud will be investigated by the Director of Finance and Corporate Resources (now the Director of Business Enablement), or a nominated individual from Internal Audit.

You have the right to request a review of the way in which this request has been processed. Should you wish to exercise this right, you will need to contact us within 40 working days of receipt of this email.
If you remain dissatisfied on completion of the review, you have the right to appeal to the Office of the Scottish Information Commissioner and thereafter to the Court of Session on a point of law only:

Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews
Fife
KY16 9DS
Telephone: 01334 464610
www.foi.scot
or for online appeals:
www.foi.scot/appeal

Regards,
SOSE Corporate Relations
FOI@sose.scot

Appendix A

Counter Fraud Policy | 2024

Descriptor	Changes made	Date	Version	Approved By
Policy first implemented	New Policy	16 Sep 2021	1.0	Audit & Risk Committee
Review no.1	Removal of references to T&D Directorate and allocation of responsibilities to appropriate members of staff. Changes to Appendix 1 Para 1.5 (reporting suspicions – addition of DPO).	10 Nov 2022	2.0	Director F&CR
Review no.2	Review at 2-year point	4 Nov 2024	3.0	Director F&CR
Review no.3				
Review no.4				
Review no.5				
Review no.6				

Name of policy being superseded (if applicable)	
Related policies	Delegated Authority Policy
Related SOPs	
Related Guidance	
Equality Impact Assessment completed	
Intended Audience	All SOSE Staff
Team responsible for policy	Governance and Assurance Team
Policy owner contact details (email)	Executive Director F&CR
Approved by	Audit & Risk Committee for major changes and Executive Director F&CR for regular or minor updates
Additional points of contact	DPO, Head of Governance & Assurance [redacted]
Policy due for review (date)	10 November 2026

Contents |

1.0 Introduction |

1.1 SOSE is committed to applying the highest standards of ethical conduct and integrity in our business activities. We take a zero-tolerance approach to fraud, bribery and corruption and are committed to acting fairly, professionally and with honesty in all our business dealings and relationships wherever we operate and to implementing and enforcing effective systems to counter fraud, bribery, and corruption.

1.2 At all times all staff are required to act honestly and with integrity, and to safeguard the public resources for which they are responsible.

1.3 Fraud is an ever-present threat to these resources and hence must be a concern to all SOSE staff who are key to our frontline defence. Fraud or attempted fraud is seen as a very serious matter and will lead to disciplinary action being taken against employees, potentially leading to dismissal, and /or to legal action against all individuals or corporate entities involved in the fraud or potential fraud.

1.4 SOSE is committed to ensuring full compliance with all anti-fraud, bribery and corruption laws and regulations in respect of our conduct. In Scotland anti-fraud relies on the common law, such as case law, judicial precedent etc. In addition, the following legislation is relevant:

- Bribery Act 2010
- Digital Economy Act 2017
- Criminal Finances Act 2017
- Anti-Money Laundering Act 2018
- Data Protection Act 2018 (implementing General Data Protection Regulations (GDPR))

1.5 The following other guidance and policies are also relevant:

- Framework Agreement between Scottish Government and SOSE
- Scottish Public Finance Manual
- SOSE policies, in particular:
  - Whistleblowing Policy
  - Code of Conduct
  - Disciplinary Policy
  - Conflicts of Interest Policy
  - Information Security Policies and associated guidance
- SOSE Gifts and Hospitality Guidance
- SOSE guidance, including processes for payment release

1.6 A detailed **Response Process** is in place which outlines the process followed where there are any suspicions of attempted fraud. This is attached at **Appendix 1** to this document. Key to this is vigilance and the importance in reporting any concerns or suspicious activity as soon as possible. All concerns will be taken seriously, and appropriate action will be taken to address any control weaknesses noted.

1.7 This policy will be subject to regular review to reflect changes in legislation or internal processes and at least every two years.

2.0 Policy Statement |

General

2.1 The public expects high standards of personal integrity from public servants, including all SOSE employees. This policy sets out SOSE's corporate view on fraud; emphasises our zero-tolerance approach; and summarises key responsibilities. A separate response plan (Appendix 1) provides details on how to report concerns and what action will be taken.

2.2 The SOSE Board and Senior Leadership Team are committed to good governance and to implementing and enforcing effective systems throughout the organisation to prevent any improper conduct arising in our business dealings. Whilst detected fraud (internal and external) within SOSE is rare, it does happen, and the controls endorsed by the Board and Leadership Team are in place to ensure we continue to address any weaknesses in process or systems.

2.3 SOSE is specifically required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud.

2.4 SOSE is committed to ensuring opportunities for fraud are minimised. This policy outlines the approach to prevention, detection, reporting and handling of fraud. Throughout this document we use the term 'fraud' to refer to all misuse, including bribery and corruption and cyber attempts.

Policy Application

2.5 The policy applies to all persons working on behalf of SOSE in any capacity, including employees at all levels and grades; Board members including co-optees; agency works; seconded workers; agents; volunteers; placements such as graduates, interns or modern apprentices; contractors; consultants; third party representatives; partners; and sponsors.

2.6 In this policy "third party" means any individual or organisation you come into contact with during the course of your work for SOSE and includes: actual and potential clients; customers; suppliers; advisors; business contacts; other public bodies, including their advisors, representatives, and officials; politicians and political parties.

Aim of the Policy

2.7 This policy aims to:

- Promote a culture of integrity, honesty, and professionalism, recognising that staff maintain these fundamental values in their approach to work, especially embodying one of SOSE's four core values of being responsible
- Set out responsibilities in observing and upholding SOSE's position on fraud
- Outline the process to those working for SOSE on how to recognise, respond to and report fraud, bribery, corruption or other financial control issues

Objectives and Culture for Countering Fraud

2.8 SOSE has five strategic objectives in our approach to countering fraud:

- **Awareness:** Raising awareness and use of safeguards which can be put in place
- **Prevention:** Improving our systems and controls to support our business and services

- **Teamwork:** Working together with Scottish Government and other organisations to share information and develop combined approaches to countering fraud
- **Investigation:** Proactivity in analysing data to identify areas at risk, by being effective and professional in our investigations of specific cases and by maintaining a robust whistle blowing procedure
- **Enforcement:** Supporting the appropriate authorities in law enforcement

2.9 Our approach aims to ensure a zero-tolerance culture is maintained and the risk of fraud is effectively managed at all levels of service delivery by:

- Committing to clear ethical standards through a formal counter fraud policy
- Communicating our attitude to fraud by raising awareness of our counter fraud policy to all staff
- Supporting all staff in their responsibilities in preventing and detecting fraud through guidance and training
- Providing managers with specialist support in designing, operating, and reviewing internal controls
- Maintaining comprehensive procedures for preventing and detecting fraud that are carefully followed and monitored
- Protecting members of staff through a robust process for reporting suspicions of fraud
- Responding to fraud effectively through a comprehensive fraud response plan
- Using the data and technology which we have in place efficiently to combat fraud
- Sharing knowledge of vulnerabilities and lessons learned through strong communication channels

Legal Recourse

2.10 Fraud is a criminal offence and may lead to proceedings in the civil and criminal courts. In Scotland it is prosecuted as a common law offence and so penalties would be on a case-by-case basis.

2.11 Under the Bribery Act 2010, individuals found guilty of bribery, tried as a summary offence (i.e. one that does not require a judge and jury) may face up to 12 months years imprisonment and/or a fine of up to £5k. Someone found guilty on indictment (i.e. a more serious offence, with a decision by the high court and judge and jury) faces up to 10 years imprisonment and an unlimited fine. If SOSE is found to have taken part in, or failed to prevent bribery, we can face an unlimited fine and face damage to our reputation.

2.12 Under the Criminal Finances Act, penalties for the offences include unlimited fines and ancillary orders such as confiscation orders.

2.13 SOSE therefore takes its legal responsibilities very seriously.

3.0 Key Definitions |

General

3.1 This policy covers fraud, including cyber attempts, bribery, and corruption. The following outlines what is meant by each. Examples of fraudulent activities are included at Appendix 2.

What is Fraud?

3.2 Fraud is the use of deception with the intention of obtaining personal gain, avoiding an obligation of causing a loss to another party. It can be used to describe a wide variety of dishonest behaviour such as forgery, false representation, and concealment of material facts. The use of IT resources is included where its use is a material factor in carrying out a fraud.

3.3 Fraud can be committed in a number of ways however always results in a gain for an individual or others, or causing a loss to others, including:

- **Common Law Fraud:** Where an individual carries out any Pretence (falsehood or deceit) intending to Induce the deceived person to do something to his or another person's (and organisation's) prejudice
- **Uttering:** Where an individual tenders 'as genuine' a forged document or a genuine document in false circumstances and causes the deceived person to do something to his or another person's (and organisation's) prejudice
- **Embezzlement:** Where the appropriation of property without the consent of the owner takes place, where a person has received a limited ownership or possession or control of the property, subject to restoration at a future time, or possession of property subject to liability to account for it to the owner - very often referred to as a 'Breach of Trust'

3.4 SOSE can be exposed to:

- **External Fraud:** Perpetuated by individuals outside the organisation
- **Internal Fraud:** Perpetuated by employees, including management and non-executive members
- **Collusion:** Either within SOSE or between employees and individuals outside the organisation

3.5 **Case Study 1 – External Fraud (Third Party Client):**

- *An account managed client submits a fictitious invoice to support evidence for release of SOSE funding*
- It is an offence for a client to submit a false claim for the purposes of making a financial gain. SOSE procedures specify that sufficient evidence is held prior to the release of funds.

3.6 **Case Study 2 – External Fraud (Own Hand Project):**

- *A contractor submits an invoice for payment for work that has not been undertaken or completed*

- SOSE processes should ensure that invoices are supported by appropriate evidence of work undertaken and that appropriate verification checks take place before payments are made.

3.7 **Case Study 3 – Internal Fraud:**

- *Your Line Manager asks you to process a payment to a different bank account for a client organisation without any back-up for a change in details for the claim*
- Bank details of a client should not be amended unless formally requested by the client. You should not be pressurised into doing anything with which you are not comfortable is legal. It is an offence for an individual to use their position with a view to making a gain for themselves.

3.8 **Case Study 4 – Collusion:**

- *You knowing accept forged invoices as evidence for a claim from a client*
- It is an offence for you to knowing accept forged invoices from an account managed client for the purposes of facilitating a payment to them.

What is Cyber Fraud?

3.9 Cyber fraud is the use of the internet to get money, goods, etc. from people illegally by deceiving them. It also describes a situation in which someone uses the internet to get money, goods, etc. from people illegally by tricking them.

3.10 Cyber fraud is mainly managed by procedures Enterprise IS (EIS) have in place; however, managing against cyber fraud also requires the vigilance of employees.

3.11 **Case Study 5 – Cyber Fraud:**

- *An email purporting to be from a supplier is received requesting payment to be made to new bank details*
- SOSE has detailed procedures to be followed for amending any supplier detail. The SOSE Finance Team will not amend any details on the basis of an email received this way.

3.12 **Case Study 6 – Cyber Fraud:**

- *The SOSE Chief Executive emails you direct requesting an urgent payment be made*
- The SOSE Chief Executive would not request payment in this way. Normal procedures would be followed in approving payments to suppliers and clients, including receipt of invoices and claim documentation.

What is Bribery and Corruption?

3.13 Bribery is offering, promising, giving, or accepting any financial or other advantage, to encourage the recipient or any other person to perform their functions or activities improperly, or to reward them for acting improperly.

3.14 An advantage includes money; gifts; loans; hospitality; services; discounts; award of contracts; or anything else of value.

3.15 Corruption is any abuse of a position of trust to gain an unfair advantage and includes both corrupting someone else and being corrupted oneself.

3.16 A person is deemed to act improperly where they act illegally, unethically, or contrary to an expectation of impartiality or good faith, or where they abuse a position of trust. The improper acts may be in relation to:

- Any business or professional activities
- Activities in the course of employment
- Other activities by or on behalf of an organisation of any kind.

3.17 **Case Study 7 – Bribery and Corruption:**

- *A supplier gives your family member a job but makes it clear that in return they expect you to use your influence in our organisation to ensure that we do business with them*
- It is an offence for a supplier to make such an offer. It would be an offence for you to accept the offer as you would be doing so to gain a personal advantage.

3.18 **Case Study 8 – Bribery and Corruption:**

- *The Director of a client organisation offers you tickets to a major sporting event and request that, in exchange, you use your influence to ensure that their application for grant assistance is approved*
- It is an offence for the Director to make such an offer. It would be an offence for you to accept the offer as you would be doing so to gain a personal advantage.

What are Facilitation Payments?

3.19 Facilitation payments are more commonly referred to as 'back-handers' or bribes and are unofficial payments made to exert influence to effect a particular outcome.

3.20 You must avoid any activity that might lead to a facilitation payment being made or accepted by us or on our behalf, or that might suggest that such a payment will be made or accepted. If you are asked to make a payment on our behalf, you should always be mindful of what the payment is for and whether the amount requested is proportionate to the goods or services provided. You should always ask for a receipt which details the reason for the payment.

3.21 SOSE does not make, and will not accept, facilitation payments of any kind.

What is Money Laundering?

3.22 Money laundering is the concealment of the origins of illegally obtained money, typically by means of a complex sequence of transfers involving foreign banks or legitimate businesses.

What is Theft?

3.23 Theft is the wrongful appropriation of the property of another, with the intention permanently to deprive that other of possession.

3.24 SOSE will take action where any theft has been identified, including recovery of items and reporting to police.

4.0 Gifts and Hospitality |

General

4.1 The Bribery Act 2010, states that it is a criminal offence for anyone to give or receive any financial or other advantage to encourage that person to perform their functions or activities improperly or to reward that person for having already done so. The penalties for criminal offences in this area are severe – individuals can face fines and/or a prison sentence (of up to 10 years) and organisations can face unlimited fines.

4.2 SOSE has a zero-tolerance approach to any attempts at bribery (giving or receiving of anything which may be deemed as an incentive) by or for its employees and encourages all employees and associated persons to report any suspected bribery activity immediately. This should be raised immediately with their people manager (also see the Whistleblowing Policy for details on raising any concerns.

4.3 Given this zero-tolerance approach, all new employees will be required to complete mandatory training on bribery as part of their induction to SOSE.

4.4 Third parties can also potentially present SOSE with risks and they must be advised of the existence and operate at all times in accordance with this policy.

4.5 Below provides more detailed guidance on the areas of hospitality and gifts. This guidance applies to spouses, partners, or other associates of an employee, if it can be argued or perceived that the gift or hospitality is, or is intended to be, received on behalf of an employee.

Receipt or Provision of Hospitality and Gifts [see also the SOSE Gifts and Hospitality Policy]

4.6 Employees should not misuse their official position or information acquired in the course of their official duties to further their private interests or those of others. They should not receive or provide benefits of any kind from or to a third party which might reasonably be seen by members of the public to compromise their personal judgement and integrity. As outlined above, it is a serious criminal offence for employees to receive, agree to accept or attempt to obtain any gift, or consideration for doing, or not doing, anything or showing favour, or disfavour, to any person in their official capacity.

5.0 How SOSE Limits Exposure to Fraud |

General

5.1 SOSE has strong internal control arrangements, supported by good record keeping, which helps:

- Create an environment which limits the possibility of fraud occurring
- Minimise the opportunity for fraud to occur
- Ensure appropriate evidence to support the legitimacy of SOSE activity and payments

5.2 These arrangements are both preventative, designed to limit the possibility of fraud occurring, and detective, designed to spot errors, omissions, and fraud after it has occurred. Controls in place have been designed to ensure they are proportionate to the risk involved.

5.3 Where new systems or products are being designed, the risk of fraud will always be considered, and appropriate controls agreed with management. Controls include segregation of duties;

password controls; supervisory checks; and reconciliations. SOSE has a low-risk appetite for fraud.

Segregation (or Separation) of Duties

5.4 Allocating responsibility for too many functions to one person should be avoided. The risk of fraud can be reduced through ensuring proper separation of duties so that one person cannot be involved in all stages of a transaction and/or activity. This includes due diligence on investment proposals and approvals thereof, and ordering, receipt and authorising of payments for goods and services.

5.5 Without adequate separation of duties, the effectiveness of other control measures is undermined.

5.6 In SOSE the separation of key functions forms an integral part of systems design and control and is essential in minimising the scope for irregularity. Where separation of duties is not possible, for example where there are limited available resources, alternative management controls should be in place. These may include management reconciliations, exception reporting etc.

Financial Transactions Controls

5.7 SOSE has defined procedures for the processing of financial transactions including awarding contracts; authorising grants; creating and amending standing data for clients, suppliers, and employees; and making payments for goods, services, or claims.

5.8 It is key that:

- There is adequate separation of duties and proper authorisation processes for payments
- Staff who require to adhere to these procedures are familiar with them and/or are aware of who to contact with queries
- Accounting and other records such as cash and bank balances, stock counts and asset registers are regularly reconciled to confirm the position
- Staff who are bankrupt or insolvent have alerted their line manager who will consider if the individual should continue to hold the same responsibilities or if additional monitoring is required
- Access to, and creation and amendment of, financial and HR records be limited
- All accounts, invoices and records relating to dealings with third parties, including suppliers and clients, are prepared promptly and not kept "off- book"

National Fraud Initiative (NFI)

5.9 SOSE is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds, un order to prevent and detect fraud.

5.10 Audit Scotland is responsible for carrying out a biennial data matching exercise known as the National Fraud Initiative (NFI). SOSE takes part in this as a means to assist in the prevention and detection of fraud. A computerised data matching exercise is undertaken whereby SOSE records are compared to records held by other participated organisations and also within our own systems to see how far they match.

5.11 In taking part in the NFI, SOSE is able to have a 100% check undertaken on our records to allow potentially fraudulent claims and payments or errors to be identified. Where a match is identified it indicates an inconsistency that requires further investigation. SOSE takes a proportionate approach to undertaking these further investigations and ensures any control issues are addressed. No assumptions can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

5.12 More information can be found at https://www.audit-scotland.gov.uk/our-work/counter-fraud

Collaboration Activity

5.13 SOSE is increasingly involved in collaborative activity in delivery of our strategic priorities. We work with our Partners in ensuring appropriate controls are in place to minimise exposure to risk of fraud.

5.14 Where any concerns are identified in such activity, investigations will be undertaken collaboratively.

Monitoring Arrangements

5.15 Many instances of fraud are due to failure to comply with existing controls. Good control systems are, therefore, supported by appropriate monitoring arrangements to prevent and detect fraud.

5.16 Managers have key responsibility for ensuring sound controls are in place, procedures have been disseminated to key individuals and controls are operating effectively as intended.

5.17 Internal and external audit, and other assurance mechanisms, undertake regular independent assessments on the adequacy of controls in place. In addition, internal audit should be consulted where system changes are proposed to ensure no loss of controls.

5.18 Updates are provided to Auditors, the Audit and Risk Committee and to the Scottish Government through provision of Committee papers and through meetings with Sponsor Team.

6.0 Roles and Responsibilities |

General

6.1 At all times all staff are required to act honestly and with integrity, and to safeguard the public resources for which they are responsible. Staff should remain vigilant and alert to the possibility of fraud or error and act in accordance with the Fraud Response Process (Appendix 1) where any concerns are noted.

6.2 Key is to act promptly and to ensure evidence is not compromised, for example by undertaking any investigations prior to reporting concerns and/or suspicions. Where an investigation is being undertaken, staff should ensure cooperation with whoever is undertaking the exercise. At all times confidentiality will be retained insofar as possible.

6.3 In addition to the general roles noted above, specific responsibilities of key groups are detailed below.

Roles and Responsibilities – Chief Executive

6.4 The Chief Executive is responsible for establishing and maintaining a sound system of internal control that supports the achievement of the overall SOSE strategic objectives. The role also includes:

- Accountable Officer promotion to highlight importance of fraud prevention
- Consideration of proportionate controls to ensure fraud risk is managed
- Maintaining oversight of serious fraud investigations
- Reviewing reports provided by the Director of Finance and Corporate Resources or Internal Audit on fraud matters.

Roles and Responsibilities – Management

6.5 Management including Senior Leadership Team and Senior Management Team are responsible for:

- Day to day prevention and detection of fraud
- Development and maintenance of effective systems of control
- Identifying risks to which systems, operations and procedures are exposed
- Ensuring controls are complied with
- Reporting in line with the Fraud Response Process any suspicions of irregular or improper behaviour or fraud which have been reported to them
- Ensuring no compromise of evidence through undertaking investigations prior to reporting suspicions
- Supporting staff who raise concerns.

Roles and Responsibilities – All Staff

6.6 Every member of staff is responsible for:

- Acting with honesty and integrity in the use of public resources
- Conducting themselves in accordance with the Code of Conduct
- Being alert to the possibility of fraud
- Reporting details immediately in line with the Fraud Response Process if there are any suspicions of fraud
- Cooperating with investigations and/or reviews.

Roles and Responsibilities – Director of Finance and Corporate Resources

6.7 The Director of Finance and Corporate Resources (Director F&CR) is a key individual in the implementation of the fraud policy and is the key contact for reporting suspicions as per the Fraud Response Process.

6.8 Specific responsibilities of the Director F&CR and the wider directorate, which includes Legal are:

- To be the key contact for the reporting of concerns

- Assisting in the prevention of fraud by reviewing and reporting on the effectiveness of the internal control system
- Providing advice and guidance on control issues and supporting new system development
- Impartially investigating allegations of fraud and reporting findings to SLT, Internal Audit and ultimately the Audit and Risk Committee
- Assisting in the assessment of whether a prima facie instance of fraud has occurred
- Onward reporting of fraud to relevant third parties including, but not limited to, Scottish Government, Audit Scotland, and Police Scotland
- Periodically reviewing the fraud policy and fraud response plan
- Advising on and supporting any recovery action
- Acting as Fraud Liaison Officer for SOSE.

Roles and Responsibilities – Human Resources Manager

6.9 The Human Resources Manager is responsible for:

- Reporting to, and liaising with, the Director of Finance and Corporate Resources in any investigation involving allegations against staff
- Ensuring process is followed in relation to this policy and other relevant policies, such as Whistleblowing Policy
- Ensuring strong controls are in place and are followed for creation, amendment, and deletion of employee records
- Monitoring the investigation process for compliance with HR policies and ensuring appropriate segregation of duties in the investigation process.

7.0 Identifying Fraud

General

7.1 It is not always easy to identify fraud. Often suspicion may be raised but is not acted on and reported. Fraud is often committed where the following is true:

- There is **opportunity** through weak internal controls and access to assets, including information, allows fraud to occur
- An individual **rationalises** their behaviour for a variety of reasons
- There is a **motivation** or need for undertaking such activity, such as financial factors.

7.2 If you are unsure about whether a particular action constitutes fraud or attempted fraud, the matter should be raised with your line manager and/or the Director of Finance and Corporate Resources who will consider what action is required. Where the concern is related to a cyber attempt, EIS should be informed promptly, and they will ensure appropriate action is taken.

What to be Aware Of – 'Red Flags'

7.3 There are a number of fraud indicators or 'red flags' which could give cause for concern. Whilst these are indicators, there may be reasonable explanation and therefore should be reported in line with the **fraud response process** as outlined at Appendix 1.

7.4 The following activities, which may be known by SOSE or brought to our attention at any stage, may be 'red flags' which could require further investigation.

7.5 Third Party Red Flags:

- Engages in, or has been accused of engaging in, improper business practices
- Has a reputation for paying bribes, or requiring that bribes are paid to them
- Insists on receiving a commission payment prior to signing a contract
- Requests payment:
    - In cash
    - Without an invoice and/or receipt
    - To a geographic location different from where they reside or conduct business
    - For an unexpected additional fee to 'facilitate' a service
    - To 'overlook' potential legal violations
- Demands lavish entertainment or gifts before commencing or continuing contractual negotiations of provision of services
- Non-standard or customised invoice
- Insists on the use of side letters and refuses to put agreed terms in writing
- Overcharging for services
- Request for use of an intermediary not known to SOSE without an appropriate agreement in place
- Offer of unusually generous gift or lavish hospitality
- Request for employment or some other advantage to a friend or relative.

7.6 Other External Fraud Red Flags:

- Photocopies of documents when originals would be expected
- Cash payments made by clients for items against which a claim is being made
- Discrepancies in information e.g. signatures and dates
- Unexpected queries from clients or suppliers, in particular where requesting changes to standing data such as bank account details
- Unwillingness to sign legal or other key documentation
- Requests for non-standard types of payment
- Unexpected trends or results e.g. from reconciliations

7.7 Internal Fraud Red Flags:

- Evidence of excessive spending by staff in cash/contract work
- Inappropriate relationships with suppliers or clients
- Reluctance of staff to take leave
- Undue possessiveness of, or anomalies between, work records
- Pressure from colleagues to avoid normal control procedures
- Abnormal Travel and Subsistence claims, overtime, or Flexible Working Hours

8.0 What To Do If You Suspect Fraud |

General

8.1 Any suspicions or allegations of fraud should be immediately reported to:

- Line Manager or Director who will escalate to Director of Finance and Corporate Resources
- Director of Finance and Corporate Resources (where suspicion relates to your Line Manager)
- The Data Protection Officer by the staff member notified of the suspicion in all cases

8.2 SOSE has a detailed **fraud response process**, attached at **Appendix 1**. This outlines what to do if you suspect a fraud. Employees are encouraged to raise concerns about any suspicion of fraud at the earliest possible stage. Where the concern is related to a cyber attempt, EIS should be informed promptly and they will ensure appropriate action is taken.

8.3 If you are unsure about whether a particular action constitutes fraud or attempted fraud, the matter should be raised with your line manager and the Director of Finance and Corporate Resources who will consider what action is required.

Dos and Don'ts

8.3 In line with the **Fraud Response Process** at Appendix 1, the following lists some simple dos and don'ts where there are any suspicions of fraud:

- **Do:**
  - Make a note of your concerns, recording all relevant details in a timely manner
  - Retain any evidence you have
  - Report any concerns and pass on all evidence you have
  - Provide support for any investigation, if required
  - Seek advice from line manager and/or Director of Finance and Corporate Resources if you are unsure
  - Seek support from Director of Transformation and Development if you believe you.
- **Don't**
  - Be afraid to raise concerns
  - Compromise evidence by investigating yourself, including approaching the individual you suspect

- Raise concerns with individuals other than those outlined in the Fraud Response Plan to ensure an objective investigation can be undertaken.

Protection

8.4 SOSE is committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in fraud or because of reporting any suspicions in line with this policy or the whistleblowing policy. If you believe you have suffered such treatment, you should inform your line manager and/or the Director of Transformation and Development and Director of Finance and Corporate Resources as soon as is possible. If the matter is not remedied, the SOSE Grievance Policy should be followed.

8.5 In so far as possible, all suspicions raised will be treated in confidence and only shared with those who are involved in the investigation.

9.0 Other Matters |

Communication and Training

9.1 All staff will receive access to information and training as appropriate on this policy. Staff communications are used to alert staff to any immediate matters which arise. Training modules are available through the Learning Pool application which all SOSE staff have access to.

9.2 At the outset of any business relationship with suppliers, contractors and business partners, our zero-tolerance approach should be communicated with them.

Breaches

9.3 In line with our zero-tolerance approach to fraud, any breach of this policy will be taken seriously.

9.4 Where any employee is considered to have breached this policy, the SOSE disciplinary policy will be followed. This could result in dismissal or other action being taken.

9.5 Where an individual or organisation working our behalf is found to have breached this policy, we would consider termination of the contract.

Lessons Learned

9.6 As part of the investigation of any concerns, the Director of Finance and Corporate Resources will seek to ensure:

- Reports outlining findings are produced promptly
- Control weaknesses are identified and addressed timeously and in a proportionate manner
- Lessons learned are captured and disseminated
- Updates are made to policy, procedures and guidance as required.

Appendix 1 to
SOSE Counter Fraud Policy
Dated November 2024

1.0 Fraud Response Process |

Purpose

1.1 The SOSE Fraud Response Plan (the Plan) sets out arrangements to ensure when fraud is suspected, effective action is taken, as appropriate, to:

- Investigate the circumstances
- Minimise the risk of subsequent loss
- Ensure appropriate recovery action is taken and/or initiate action to write off any losses
- Remedy any weaknesses in internal controls
- Capture and share any lessons learned
- Initiate disciplinary and legal procedures
- Demonstrate SOSE's zero-tolerance approach to fraud.

Application

1.2 The Process applies equally to all suspicions of fraud, bribery, and corruption. The term fraud is used to cover all such instances. It applies to both internal and external fraud and any combination thereof.

1.3 It also applies to cyber fraud attempts.

Notification - General

1.4 To ensure evidence is not compromised it is vital no investigation is undertaken by staff at the time of suspicions or allegations being noted. Any investigation by an individual could prejudice evidence through contamination, loss, or destruction.

1.5 Any suspicions or allegations of fraud should be immediately reported to:

- Line Manager or Director who will escalate to Director of Finance and Corporate Resources
- Director of Finance and Corporate Resources (where suspicion relates to your Line Manager)
- The Data Protection Officer by the staff member notified of the suspicion in all cases

1.6 Where concerns are related to any of the individuals identified above, you should exclude them from the notification process and report on to Chief Executive Officer if it relates to the Director of Finance and Corporate Resources.

1.7 Where a member of the public wishes to raise concerns or to make an allegation, they should be directed to the Director of Finance and Corporate Resources in the first instance.

1.8 SOSE also has access to a confidential anonymous reporting mechanism through the Scottish Government Fraud Response Team who receive and record information about suspected frauds, either by telephone (using the CrimeStoppers fraud hotline: **0800555111)** or in writing.

1.9 To ensure evidence is not compromised, it is vital no investigation is undertaken other than by the Director of Finance and Corporate Resources or nominated individual.

Notification - Cyber

1.10 Where the suspicion is related to cyber fraud, this should be reported via the EIS helpdesk and to the SOSE IT Team and the Data Protection Officer. Emails received should not be forwarded on.

Investigation – General

1.11 Suspected instances or allegations of fraud will be investigated by the Director of Finance and Corporate Resources, or a nominated individual from Internal Audit. All reviews will be undertaken in an independent, consistent, and impartial manner. The review will ensure it protects the interests of SOSE, the suspected individual(s) and the individual reporting the matter.

1.12 The investigation process will vary according to the circumstances in each case. However, in all cases, suspicion will not be taken as evidence or assumption of guilt.

1.13 The Director of Finance and Corporate Resources, or nominated individual, will undertake the investigation ensuring appropriate steps are taken to minimise contamination, loss, or destruction of evidence. This may include securing physical and documentary assets and records of computer use. It may also recommend restricting access to buildings.

1.14 Investigations will be undertaken promptly on reporting of suspicions to ensure evidence is gathered as quickly as possible to avoid compromise.

1.15 Where concerns are related to a member of staff, and where initial investigations are indicating reasonable grounds for suspicion, it may be appropriate to suspend an employee to allow a full investigation without prejudice. Suspension will only be undertaken in consultation with the Director of Transformation and Development who will ensure appropriate policies are followed. Again, suspension is not an implication of guilt, nor should it be regarded as disciplinary sanction.

1.16 **At no time should an individual compromise evidence by undertaking any investigation of their own.**

Confidentiality

1.17 All information received related to suspicions of fraud and/or collected as part of the investigations will be treated with the utmost confidentiality and only shared where there is a need.

1.18 Where the information relates to a member of staff, this is shared on a need-to-know basis and only in the course of the investigation. Only where there is any follow up action, for example disciplinary action, will a record be placed on the employee file.

1.19 In undertaking the investigation, the minimum number of individuals to allow the investigation to be undertaken effectively will be involved. On occasions, EIS may need to assist with specific access to computer and email records. Where this is considered appropriate, specific approval will be sought from the SOSE Chief Executive or Director of Finance and Corporate Resources.

1.20 Although SOSE will do its utmost to protect the identity of an individual who raises a concern and does not want their name disclosed, it must be appreciated that the investigation process, or a court process, may lead to disclosure of an individual's identity, therefore SOSE cannot guarantee confidentiality in such instances.

Third Party Liaison and Onward Reporting

1.21 Following investigation by the Director of Finance and Corporate Resources, and if deemed the most appropriate course of action by the Fraud Response Group (FRG), SOSE may report suspected frauds to Police Scotland for further investigation. This will be in particular for those cases of a serious or complex nature.

1.22 The Director of Finance and Corporate Resources will liaise directly with Police Scotland and provide all evidence collected in the original investigation, on request. SOSE will fully cooperate in all Police Scotland investigations.

1.23 As appropriate, a copy of the report from the Director of Finance and Corporate Resources will be provided to the SOSE Chief Executive for information. The Audit and Risk Committee are also updated at each meeting on any investigations which have concluded in period.

1.24 SOSE is required to also report details of any fraud to Scottish Government and Audit Scotland and to formally complete an annual return.

1.25 Where a previously identified fraud has resulted in legal action, regular updates on progress will be provided to the Audit and Risk Committee, Scottish Government and Audit Scotland.

Recovery Action

1.26 The report from the Director of Finance and Corporate Resources will identify if SOSE has suffered any loss from the fraud. Following discussion and agreement by the FRG, SOSE will take steps including legal action if appropriate, to recover any losses arising.

1.27 SOSE will also consider what actions are required to prevent a recurrence.

Follow up action

1.28 Any lessons learned in the course of an investigation will be included in the report from the Director of Finance and Corporate Resources. In line with normal audit process, recommendations made will be followed up to ensure appropriate action has been taken.

1.29 Where internal control refinements are required, these will be implemented as soon as possible, and normal control checks will be undertaken to ensure operating effectively and as intended.

Appendix 2 to
SOSE Counter Fraud Policy
Dated November 2024

1.0 Examples of Fraudulent Activities |

1.1 **Travel Subsistence and Personal Allowances:**

- Claims for journeys not made
- Overstated claims
- Claims relating to circumstances that no longer apply
- Forged or false receipts

1.2 **Pay or Allowances Paid Via Payroll:**

- The creation of fictitious employees on the payroll
- False claims such as for overtime and other allowances
- Failure to declare known payroll overpayments
- Unauthorised changes to payroll data
- Deliberate failure to repay advances or overpayments of salary
- Misuse of pay advances or loans (e.g. season ticket advance used for purpose other than that intended)

1.3 **PERSONNEL MANAGEMENT:**

- Staff not recording annual leave or other absences
- Misuse of official time, e.g. internet abuse
- Deceit and misrepresentation for advantage, e.g. provision of false references or qualifications to secure employment or promotion

1.4 **Theft of:**

- Petty cash
- Equipment
- Information

1.5 **Exploitation of Assets and Information:**

- Using official vehicles for personal gain
- Running a private business using SOSE assets (e.g. IT system)
- Selling information to marketing companies or other entities
- Failure to declare a conflict of interest and gaining benefit as a result

1.6 **Procurement:**

- Manipulating tenders/collusive tendering
- Rigging specifications in favour of one supplier

- Bid rigging by suppliers via collusion with competitors
- Failure to declare a conflict of interest in relation to suppliers
- Theft of new assets before delivery to end user and before addition to asset register
- Submission of false or duplicate invoices for goods or services not provided, or for interim payments in advance of entitlement
- Goods or services ordered for personal use
- Corruption or attempted corruption of SOSE staff
- Receiving personal benefits ("kickbacks") from awarding contracts
- Failure to request payments
- Ghost companies submitting bids
- Awarding contracts out-with agreed procurement processes to the same company
- Multiple contract variations proposed by a supplier for no reason

1.7 **Payment Fraud:**

- Creating false payments
- Providing confidential information to others enabling them to make fraudulent claims
- False accounting
- Manipulation of BACS payment data
- Submission of bogus invoices
- "Phishing" attacks to obtain information to get unauthorised access to staff, supplier or corporate bank accounts
- Goods or services paid for on Government procurement cards for personal use
- Forged or false receipts

1.8 **Income Related:**

- Theft of income, e.g. interception of cash and cheques
- Understatement of, or failure to record, income so that the surplus income can be stolen
- Manipulation of fees, charges, or sales records.