

## Counter Fraud Policy

<b>Owned and maintained by:</b>	Human Resources
<b>Date checked/created:</b>	June 2019
<b>Next review date:</b>	June 2021

1. This policy sets out our approach to preventing, investigating and reporting fraud. All staff must ensure they are familiar with this policy. Audit Scotland takes a zero tolerance approach to fraud including bribery and corruption.
2. Fraud is a common law offence in Scotland and therefore does not have a legal definition. However, the Fraud Act 2006 provides a useful definition which should be referred to. A person commits a fraud if they intend to make a gain for themselves or another, cause loss to another or to expose another to a risk of loss by:
  - dishonestly making a false representation;
  - dishonestly failing to disclose to another person information which they are under a legal duty to disclose; or
  - dishonestly abusing a position that they occupy in which they are expected to safeguard, or not to act against, the financial interests of another person.
3. Audit Scotland requires a standard of absolute honesty and integrity from its staff. Trust is an essential part of this process and there is no room for dishonesty, either within Audit Scotland or with its clients or stakeholders. This approach has been endorsed strongly by Audit Scotland's Board, which requires that all fraud investigations be reported to it via the Audit Committee.
4. Audit Scotland subscribes to the principles outlined in the Scottish National Fraud Initiative (NFI) instructions and the associated privacy notices. We will include data on our staff as part of the NFI exercise. Further information on the National Fraud Initiative is available from our intranet and external website. This policy should be read in conjunction with:
  - Audit Scotland's Code of Conduct
  - Scheme of Delegation and Financial regulations
  - Information security management policy and Information Acceptable Use policy
  - Whistleblowing Policy
  - Disciplinary Policy
  - Grievance Policy
  - Ethical Standards Policy.

- 
5. Copies of these documents are located in Audit Scotland's Staff Handbook within ishare and are also available from Human Resources.
  6. This policy requires Audit Scotland employees to report any instance of suspected fraud to their Director or Audit Director. Where staff do not understand any aspect of the policy, they should seek clarification from their Director or Audit Director.
  7. All staff are required to read and agree to Audit Scotland's Code of Conduct annually. This includes disclosing any potential conflicts of interest. The Compliance Partner/Compliance Manager is responsible for reviewing all disclosures and addressing any conflicts that arise.
  8. Educational information may be issued to staff from time to time by Audit Scotland concerning fraud prevention by way of briefing notes, training programmes or ad-hoc advice. The Board and Management Team strongly support the counter fraud efforts of Audit Scotland. Please ensure you take note of any guidance issued and raise any queries or concerns with your line manager.
  9. It is important to be clear that, as an employee of Audit Scotland, you have stewardship responsibilities for any property and information of Audit Scotland and/or the bodies we audit entrusted to you and under your control. This property and information must be safeguarded from inappropriate access, loss or theft.
  10. It must also be recognised and accepted that fraud is possible in our organisation. If this is not recognised or accepted, then it is unlikely that fraud will be identified even if it is evident. Symptoms of fraud are frequently viewed as administrative errors because staff cannot believe that a colleague could possibly have committed such an act, particularly where affiliation has developed over a long period of time. Therefore, you should consider the following to help reduce the risk of any impropriety:
    - Identify property for which you have responsibility e.g. computers, flashdrives, audit files (including those in archive), departmental expenditure, supplies and company cars.
    - Identify risks associated with safeguarding this property and information. Ask yourself:
      - How could this property or information be misused or improperly used?
      - If this property or information were misused or misappropriated, how would I know?
      - What controls exist to prevent or detect inappropriate use or loss of property or information?
      - What additional controls are necessary to ensure the property or information is adequately protected from loss?
      - Is the cost of these additional controls reasonable in relation to the risk involved?
    - Establish a positive control environment in your department. It is important to demonstrate control consciousness – interest and concern for internal control should be communicated to all staff members. Ensure that an adequate system of internal control exists within your department. The key points to consider are:
      - separation of duties

- 
- physical safeguards over property
  - proper documentation and authorisations
  - adequate supervision e.g. independent checking of key transactions.
11. Audit Scotland aims to recruit honest employees. The degree of background checking is dependant on the level of accessibility to significant Audit Scotland assets. Certain information available from background and security checks is classified as personal, sensitive and / or confidential. This means that access to this information is restricted and it must be held in a secure manner. Human Resources lead on security and background checks<sup>1</sup> which is why you should speak with them prior to any formal checks being undertaken.

### **What should you do if you suspect fraud or corruption, or that ‘something is wrong’?**

12. Staff are often the first to realise there may be something seriously wrong. However, they may not express their concerns because they feel to speak up would be disloyal to colleagues or to Audit Scotland. Staff may also fear harassment or victimisation so feel it is easier to ignore the concern rather than report what may just be a suspicion of malpractice.
13. Audit Scotland’s Whistleblowing Policy is intended to encourage staff to report concerns via Audit Scotland’s procedures rather than overlooking a problem. The Board is committed to acting on all reports of suspected fraud and corruption both from within Audit Scotland and across the public sector.
14. Be assured that there will be no recriminations against staff who report reasonably held suspicions. Victimising or deterring staff from reporting any concerns is a serious disciplinary matter. Any contravention of this policy should be reported in accordance with Audit Scotland’s Disciplinary and Grievance Policies.
15. Abuse of this policy by raising malicious allegations could be regarded as a disciplinary matter.
16. If you have good reason to suspect a colleague, contractor or other person of fraud or an offence involving Audit Scotland or an audited body you should discuss it first with your manager. If you suspect your manager, you should go to the next most senior person above them in accordance with Audit Scotland’s approach in the Disciplinary and Grievance Policies. Alternatively you have the option to:
- Discuss the matter confidentially with the Chief Operating Officer; or
  - Advise the Chief Operating Officer anonymously of your concerns.
17. You may find it helpful to read Audit Scotland’s Whistleblowing Policy which provides further information.
18. If you and your manager decide between you that your suspicion may be justified, the matter must be reported to the Chief Operating Officer. Audit Scotland will then take the appropriate action, as follows:

---

<sup>1</sup> Some security vetting and background checks for employees involved with certain clients or work are undertaken by external bodies instead of our HR team. Senior management in each business group should liaise with the HR & OD Manager prior to any such checks being commissioned.

- 
- Implement its Fraud Response Plan.
  - Refer the matter to the Audit Committee.
  - Refer the matter to the Police, if appropriate.
  - Report back to the Audit Committee in all cases.
19. Do not approach the individual(s) about whom you have concerns and do not discuss the matter with anyone else.