Fraud Response Policy

Manager Responsible for Review: **Director of Finance & Systems**

Method of Approval: **Audit & Risk Committee**

Date Approved: **14th October 2025**

Next scheduled Review Date: **October 2026**

Contents

1.0 Introduction

1.1 The purpose of this policy is to detail how the Guild of Students (the Guild) will respond in the event of a suspected fraud or financial irregularity. The policy seeks to define key responsibilities of staff/trustees and clarify the necessary reporting requirements.

1.2 The policy seeks to:

- Enable the Guild to prevent further losses
- Establish and secure any necessary evidence to support disciplinary and/or criminal action
- Undertake an appropriate investigation
- Recover losses where possible
- Notify relevant parties

1.3 The 'Fraud Act 2006' defines fraud as '*a dishonest act, through false representation, failure to disclose information or abuse of position, with the intent of causing a gain for self, or loss to another'.*

The criminal act is the intent and attempt to deceive and therefore attempted fraud should be treated as seriously as accomplished fraud.

1.4 The Guild is committed to the prevention of fraud and the promotion of an anti-fraud culture.

1.5 The Guild operates a zero-tolerance attitude to fraud and requires staff to act honestly and with integrity at all times, and to report all reasonable suspicions of fraud.

1.6 The Fraud Response Policy supplements the Guild's Whistle Blowing Policy contained in the Staff Handbook. The Staff Handbook can be accessed in the documents section of your 'Staff Savvy' login or available upon request from the Guild's People & Administration Department.

1.7 In addition, the Fraud Response Policy also supplements the Guild's Anti-Bribery Policy, and this policy should also be considered when fraud arises as a result of potential bribery.

1.8 The Fraud Response Policy primarily refers to potential fraud in relation to staff. However, this policy is applicable to all office bearers in relation to Guild activities, including employees, trustees, Officers and student volunteers (e.g. student group committee members and group members).

2.0 Initial Action

2.1 It is the duty of all members of staff to report any actual or suspected incidents of fraud or irregularity directly to the Chief Executive and People & Administration Manager as soon as possible.

2.2 Depending upon the nature and potential severity of the incident reported, the CEO and People & Administration Manager may convene a meeting of a Fraud Response Group to decide on an initial response and course of action.

The Fraud Response Group may consist of:

- Chief Executive
- People & Administration Manager
- Director of Finance & Systems
- Other members of the senior management team as deemed appropriate (e.g. Director of Operations, Director of Engagement, Director of Community & Representation)

2.3 The Fraud Response Group will decide upon the initial course of action although this will be dependent upon the circumstances and scale of the suspected incident. The decision of the group to initiate a fraud investigation should include consideration of:

- The most appropriate internal lead investigator to conduct the process
- The use and identification of external specialists to conduct the investigation, potentially including University Internal Audit (if deemed appropriate)
- The need to include internal specialist support, for instance from Finance, IT or Facilities.
- The need to consult legal advice, either via University Legal Services or the Guild's external solicitors.
- Identification of stakeholders that may require early notification and progress updates including if/when the police should be notified (see section 4)

3.0 Preventing Further Losses

3.1 The Guild will investigate all instances of actual, attempted and suspected fraud committed by staff, students, suppliers and other third parties, and will seek to recover funds and assets lost through fraud. Perpetrators will be subject to disciplinary and/or legal action.

3.2 Where an initial investigation provides reasonable grounds for suspecting a member(s) of staff of fraud, the Fraud Response Group will decide how best to prevent further loss. This will most likely be in consultation with the police and external/University legal advice.

3.3 It may be necessary to carefully plan the timing of a suspension in order to prevent the loss of evidence through the suspect either removing or destroying evidence. The suspension should be conducted in accordance with the Guild's HR procedures and may include preventing the suspect having access to physical spaces, assets or files (both manual and electronic). It may also be important to prevent the suspect communicating with other colleagues.

3.4 In such circumstances, the suspect may need to be approached unannounced and require close supervision whilst being escorted from the premises. The suspect should be able to retrieve personal belongings although must not be allowed to access or remove any Guild assets/information during this process. In addition, IT access should be withdrawn at this point.

3.5 The Guild will normally follow disciplinary procedures against any staff member who has been proved to have committed fraud or attempted to commit fraud. In addition, the Guild will also normally pursue prosecution in such circumstances. The Fraud Response Group will be responsible for initiating contact with the police and deciding if/when this is appropriate.

4.0 Recovery of Losses

4.1 The Fraud Response Group will ensure any losses are quantified in all fraud investigations and repayment of those losses will normally be sought in cases where it is economical to do so.

4.2 Where the loss is material, the Fraud Response Group should seek legal advice in relation to the recovery of losses (and associated costs), for instance through the civil courts where the perpetrator refuses to repay the losses, or in substantial fraud cases, the potential to freeze a suspect's assets through the court, pending conclusion of an investigation.

5.0 External Fraud

5.1 It is essential that employees, trustees, officers and volunteers also remain vigilant to suspected incidents of fraud or irregularity impacting the Guild from an external source. In order to improve the Guild's resilience to fraud, stakeholders should:

- Improve their awareness of fraud and the types of fraud prevalent at any one time
- Stop and think before acting
- Take action when there is an irregularity or suspicion of fraud
- Understand the Guild's *'norms'* through familiarisation with policies, procedures and processes.

5.2 In particular, employees, trustees, officers and volunteers should ensure they are familiar with the Guild's Financial Procedures Manual, Data Protection Policy and Data Security Policy.

5.3 Examples of external frauds include but are not limited to:

- Supplier communications – For example, this could include suppliers changing company information (e.g. bank account details) either via invoice or letter with the communications being sent fraudulently. When such communications are received, the details of the change should be independently verified with a telephone call using either a pre-existing contact number or number independently sourced (i.e. not using contact details from the source communication).

- Payroll - The same process applies for changes to employee personal details communicated to People & Administration and/or payroll. This should be separately verified to ensure the communication hasn't come from an external source.

- Credit Card fraud - The use of Guild credit cards must be reconciled on a monthly basis with online checks against statement balances conducted on a regular basis during the month. The Guild's Financial Procedures also restrict the storage of company card information on multiple sites. In addition, cardholders should check to ensure the payment processing method is secure, the site has a valid certificate and that no security warnings appear on the site.

- Cyber Fraud – Examples could include phishing scams and credential sharing (impersonations). Guild stakeholders should consider whom the e-mail is received from, is this a regular (known) contact? Were you expecting to receive the communication? Does the content of the e-mail look legitimate and has it been marked as spam by the e-mail filter?

- Bogus telephone calls/face-to-face contact – Where possible, the identity of '*cold-callers'* should be verified to ensure the person is who they say they are. This may include checking an ID or calling the company back using a known or independently verified telephone number.

- Contract impersonators within the Guild building – All University approved contractors should carry a university issued permit or ID badge. A Guild representative should be aware of any contractor within the building who is carrying out work/activities on their behalf and should be signed in at Reception. Guild stakeholders should remain vigilant of unknown persons and report any suspicious behaviour to Reception in the first instance.

6.0 Communications and Reporting

6.1 Whilst confidentiality is essential throughout a fraud investigation, it is also important for the Fraud Response Group to notify and communicate with a number of stakeholders. These will include but are not limited to:

- Chair of the Board of Trustees (and Chair of Audit & Risk Committee)
- President
- Guild Insurers
- Guild legal advisors
- Guild auditors
- University representatives (e.g. University Chief Financial Officer, Head of University Internal Audit and/or University Director of Legal Services)
- Police
- Charity Commission (see below)
- Related external stakeholders if necessary (e.g. Guild bankers, supplier, grant funder)

6.2 **Internal Reporting –** The Fraud Response Group must keep the Chair of the Guild's Trustee Board and Audit & Risk Committee regularly updated and produce a report once the investigation has been concluded and action taken. The report to Audit & Risk Committee should include:

- Details of the incident including the nature of the fraud, total estimated or actual losses and who committed the fraud.
- The outcomes of any disciplinary/legal actions taken
- The measures taken to improve processes and reduce/eliminate the possibility of a reoccurrence.

6.3 **External Reporting –** Depending upon the scale, severity and nature of the fraud, it may be appropriate for the Fraud Response Group to report the fraud incident to the Charity Commission as a serious incident.

Further information regarding the reporting of serious incidents to the Charity Commission is available at: https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity

7.0 Contacts and further information

If you have any queries in relation to this policy then please contact the People & Administration Manager, Director of Finance & Systems or CEO.