Strathclyde Students' Union

Strathclyde Students' Union Fraud Policy

Policy Owner: Chief Executive
Approval: Trustee Board
Effective Date: 05.05.2026
Review Cycle: Every 3 years, or following any incident
Review Date: 30th June 2027

1. Introduction

Strathclyde Students' Union ("the Union") is committed to the highest standards of integrity, openness and accountability. The Union has a zero-tolerance approach to fraud and is committed to minimising risk through prevention, detection, and proportionate response.

This Policy sets out the Union's approach to fraud and provides a framework for dealing with suspected or actual cases. A supporting Fraud Response Plan outlines the steps to be taken when concerns arise.

2. Definition

Fraud is the use of deception to secure an unfair or unlawful gain, or to avoid an obligation, resulting in loss to another party.

Examples include (but are not limited to):

- Theft or misappropriation of cash, stock, assets, or data;
- False expense claims, overtime claims, or timesheets;
- Misuse of Union property or resources;
- Collusion with suppliers, contractors, partners and funders;
- Cyber fraud (phishing, impersonation, unauthorised access);
- Altering or falsifying records, invoices, or applications;
- Bribery, corruption, or concealment of material facts.

Fraud can be committed by staff, elected officers, volunteers, students, contractors, or external parties.

3. Scope

This Policy applies to all:

- Union staff, elected officers and trustees;
- Student volunteers, society and sports club officers;

- Contractors, suppliers, and partners acting on behalf of the Union.

4. Strategic Approach

The Union's approach is to:

- **Prevent** fraud through clear policies, training, and strong internal controls;
- **Detect** fraud through vigilance, monitoring, and audit;
- **Respond** effectively to all concerns;
- **Recover** losses wherever possible;
- **Learn** from incidents and strengthen controls.

5. Prevention

Fraud is best tackled before it occurs. Preventative measures include:

- **Leadership –** Trustees, officers and senior staff must set the tone of integrity.
- **Policies & procedures –** Clear financial controls, segregation of duties, and record-keeping.
- **Recruitment checks –** References and right-to-work checks.
- **Cash & asset handling –** Secure storage, documented receipts, and audit trails.
- **Cybersecurity –** Compliance with Union IT and data protection policies including staff working offsite and/or abroad.

6. Detection

Fraud may still occur despite prevention. Everyone in the Union must stay alert to warning signs, such as:

- Unexplained discrepancies in accounts or budgets;
- Missing or altered documentation;
- Unauthorised changes to financial or IT systems;
- Lifestyle or behaviour inconsistent with income;
- Reluctance to share duties or take leave;
- Unusual supplier or payment arrangements.

Concerns must be reported immediately (see Section 8).

7. Responsibilities

- **All staff, officers and volunteers**: Safeguard Union resources, follow procedures, and report concerns.
- **Line managers**: Maintain and monitor internal controls in their areas.
- **Chief Executive (Designated Person)**: Owns the Fraud Policy, ensures investigations are conducted, and reports to the Trustee Board.
- **Trustee Board (Finance, Audit and Risk Committee)**: Provides oversight and ensures accountability.

8. Reporting Suspected Fraud

- Concerns should be reported promptly to a line manager, the Chief Executive, or the Union President.
- If inappropriate to report through these routes, concerns can be raised directly with the Trustee Board Vice Chair.
- Reports will be handled confidentially and whistleblowers will be protected in line with the Union's Whistleblowing Policy.
- Where criminal activity is suspected, the Union may notify the Police, OSCR, external auditors, Companies House or insurers.

9. Fraud Response Plan (Summary)

When a concern is raised:

1. **Initial Action** – Secure records and assess risk.
2. **Fraud Response Group** – Convened by the Chief Executive (or Deputy CEO if CEO is implicated), including relevant trustees and staff.
3. **Investigation** – Appoint an investigating officer, supported by external advice if required.
4. **Outcome** – Report findings to the Trustee Board; apply disciplinary or legal action as appropriate.
5. **External Reporting** – Notify OSCR, Police, auditors, University or insurers where required.
6. **Review** – Learn lessons and strengthen controls.

10. What to Do (and Not Do) if You Suspect Fraud

Do:

- Report concerns immediately.
- Record dates, times, and details.

- Keep copies of suspicious documents.
- Stay calm and act discreetly.

Do Not:

- Investigate yourself or confront the suspect.
- Destroy or alter evidence.
- Share suspicions with others unnecessarily.
- Contact the press or external bodies yourself.

11. Review

This Policy will be reviewed every 3 years or after any incident, to ensure fitness for purpose.

Appendix 1. Fraud Response Plan

This document should be read in conjunction with the Union's Fraud Policy.

1. Introduction

1.1 The purpose of this Fraud Response Plan ("the Plan") is to provide a clear framework for action when suspected or actual fraud arises within Strathclyde Students' Union ("the Union").

1.2 The Plan ensures a consistent, proportionate, and fair approach to investigating, reporting, and resolving fraud, while protecting the Union's assets, people, and reputation.

1.3 If any suspected fraud directly involves an officer listed in this Plan, the role will be substituted by a senior Trustee or independent nominee.

2. Initiating Action

2.1 Suspicion of fraud may arise from staff, officers, students, volunteers, auditors, or external parties. All concerns must be reported promptly, regardless of the amount involved, in line with the Union's Fraud Policy.

2.2 Initial reports should be made to the Chief Executive (Designated Person) or, if the Chief Executive is implicated, directly to the Deputy CEO or Trustee Board Chair.

2.3 The Designated Person will:

- Log the concern confidentially;
- Secure any records, assets, or data at risk;
- Consider whether immediate protective action is required (e.g. suspending access to systems, freezing bank accounts, restricting cash handling).

2.4 Where necessary, the Chief Executive (or Trustee Chair) will convene the Fraud Response Group as soon as possible.

3. Fraud Response Group

3.1 Membership will normally include:

- Chief Executive (Convener, unless implicated);
- Union President or other Full time elected officer;
- Deputy CEO;
- Trustee Board representative (From the FAR Committee);
- Other relevant staff (e.g. HR Manager, IT Manager) as required.

3.2 Responsibilities:

- Decide the nature and scope of the initial response;

- Secure records, evidence, and assets;
- Agree whether an investigation is required and appoint an Investigating Officer;
- Assess whether external parties (Police, OSCR, auditors, insurers, banks) should be notified;
- Manage communications, including with staff, students, and media;
- Set timescales and agree reporting requirements.

4. Investigation

4.1 The Investigating Officer will normally be a senior manager not connected with the matter, or an external investigator if independence is required.

4.2 Their duties include:

- Conducting fact-finding in a timely, fair, and confidential manner;
- Securing relevant records, IT access logs, and documentation;
- Interviewing relevant parties, following HR and disciplinary procedures;
- Preparing interim and final reports for the Fraud Response Group.

4.3 Where evidence indicates fraud has occurred, consideration will be given to:

- Suspension of staff or officers in line with disciplinary procedures;
- Restricting access to Union premises, systems, and assets;
- Involvement of external specialists (legal, IT forensics, auditors).

5. Concluding an Investigation

5.1 At the conclusion of an investigation, the Investigating Officer will prepare a Final Report including:

- A description of the incident and methods used;
- The value of any loss;
- People involved and responsibilities;
- Corrective actions taken;
- Recommendations to prevent recurrence.

5.2 The Final Report will be submitted to the Trustee Board (Via the Finance, Audit and Risk Committee). Where significant, novel, or reputationally sensitive, the full Board will be notified.

5.3 Disciplinary action may be taken against any staff or officer found responsible. Where volunteers or students are involved, appropriate action will be taken under Union and/or University disciplinary procedures.

6. External Reporting

Depending on circumstances, the Union may notify:

- Police – where criminal offences are suspected;
- Office of the Scottish Charity Regulator (OSCR) – in line with Notifiable Events guidance;
- External Auditors – for all cases of material fraud;
- Insurers – where claims may be required;
- Banks, IT providers, or third parties – if fraud involves their systems or data.

All external communication will be authorised by the Chief Executive or Trustee Board Chair.

7. Recovery of Losses

7.1 The Investigating Officer will ensure losses are quantified. The Union will seek to recover losses in all proven cases, including through civil recovery or insurance claims.

7.2 Legal advice may be sought to freeze assets or pursue repayment through the courts.

8. External Frauds

8.1 Where fraud is perpetrated externally (e.g. against the Union by third parties), the same procedures apply.

8.2 If there is any suspicion of collusion by Union staff, officers, or volunteers, this Plan applies in full.

9. Communications

9.1 All media or external enquiries must be referred to the Chief Executive. No staff, officers, or trustees should make independent statements.

9.2 The Union's Communications Team will prepare any press response, in consultation with the Fraud Response Group.

10. Review of the Plan

10.1 This Plan will be reviewed every 3 years or after each incident. Lessons learned will be incorporated into future revisions.

10.2 Amendments require Finance, Audit, and Risk Committee approval.

Appendix 2. Fraud Reporting Flowchart

Initial Suspicion

- Document concerns (dates, times, people, details).
- Keep/copy any documents that raised suspicion.
- Stay calm and discreet — do not investigate yourself.

Disclosure

- Report to your Line Manager in the first instance.
- If not appropriate, report directly to the Chief Executive or Union President.
- If the concern involves senior staff/officers, report to the Trustee Board Chair.

Fraud Response Group

- Convened by the Chief Executive (or Deputy CEO or Trustee Chair if CEO implicated).
- Includes relevant trustees and staff (e.g. Finance Manager, President).
- Secures evidence and agrees initial actions.

Investigation

- Investigating Officer appointed.
- Interim fact-finding carried out.
- Access restricted if necessary to protect evidence.

Outcome

- Findings reported to the Trustee Board / Finance Audit and Risk Committee.
- Disciplinary or legal action taken if fraud is substantiated.
- External reporting to Police, OSCR, auditors, or insurers where required.

Review & Learning

- Lessons learned documented.
- Internal controls strengthened.
- Policy and procedures updated if necessary.

Remember:

- Do not confront the suspected person.
- Do not destroy or alter evidence.
- Do not contact the media or external agencies yourself.