

DO NOT USE THIS COP IN PRINTED FORM WITHOUT FIRST CHECKING IT IS THE LATEST VERSION

The current version of this COP is available online via <https://warwick.ac.uk/services/gov/antifraud>. If you are reading this document in printed form, please check that the printed version number and date match the latest version online.

Anti-Fraud Code of Practice

Document Control:

COP Owner:	Chris Twine, Chief Operating Officer and University Secretary
COP Author:	Catherine McStay & Kirsty Jenkins, Head of Compliance & Assurance
Effective Date:	15 June 2026
Version Number:	V1.0
Date of Next Review:	06 October 2026
Published Location: [PDF version of COP accessible to end-users]	https://warwick.ac.uk/services/gov/antifraud
Secure location: [Word version of COP accessible only to COP Owner and Author for future edits. This is also the location where copies of previous versions are archived for future reference before changes are made.]	Fraud Management Assurance Group on Teams Via 'General' channel: 'Anti-Fraud documentation' folder.

Amendment History:

Version Number:	Effective Date:	Summary of Amendments	Authorised by (Name/Role/Date):
V1.0	15 June 2026	COP established	Chris Twine, Chief Operating Officer and University Secretary, 15 June 2026

Introduction

The University of Warwick is committed to the highest standards of integrity and accountability. Fraud and other forms of dishonesty are not tolerated, and all members of the University community are expected to act with honesty at all times. This commitment includes full compliance with relevant legislation, including the [Fraud Act 2006](#), [Economic Crime and Corporate Transparency Act 2023](#) and the associated corporate offence of [Failure to Prevent Fraud](#), which came into effect on 01 September 2025.

The University's [Anti-Fraud Policy](#) and this supporting Code of Practice (COP) applies to all members of the University community, including staff, students, Council and sub-committee members, and third parties. Together, they set out the University of Warwick's strategic approach to anti-fraud and corruption measures, documenting how the University identifies, assesses, manages and mitigates the fraud risks of the institution. Responsibilities are documented in full within the [Anti-Fraud Policy](#) (in RACI format) and within [FP3](#) (section 3.6.1) and intentionally not duplicated within this COP.

Reporting Fraud

Any suspected fraud should be reported to the University without delay:

- **Students** should raise any concerns about suspected fraud with their Personal Tutor or Head of Department.
- **Staff** should report concerns to their Line Manager or Head of Department.
- If the concern relates to the person you would normally report the suspected fraud to, you can contact the Director of Internal Audit & Assurance directly to discuss your concerns and identify the best way forward.

An alternative reporting route is through the University's [whistleblowing process](#), which allows the reporting party to remain anonymous. However, there may come a point at which anonymity cannot be maintained if the member of staff who has perpetrated the alleged fraud is to be disciplined or prosecuted and direct evidence is required from the reporter. Any disclosure of identity will always be discussed with the reporter.

If you are a Head of Department, Line Manager or Personal Tutor and a student or staff member approaches you to discuss suspected fraud, you should follow the [What should I do if someone reports a suspected fraud to me v1.0.docx](#) guidelines.

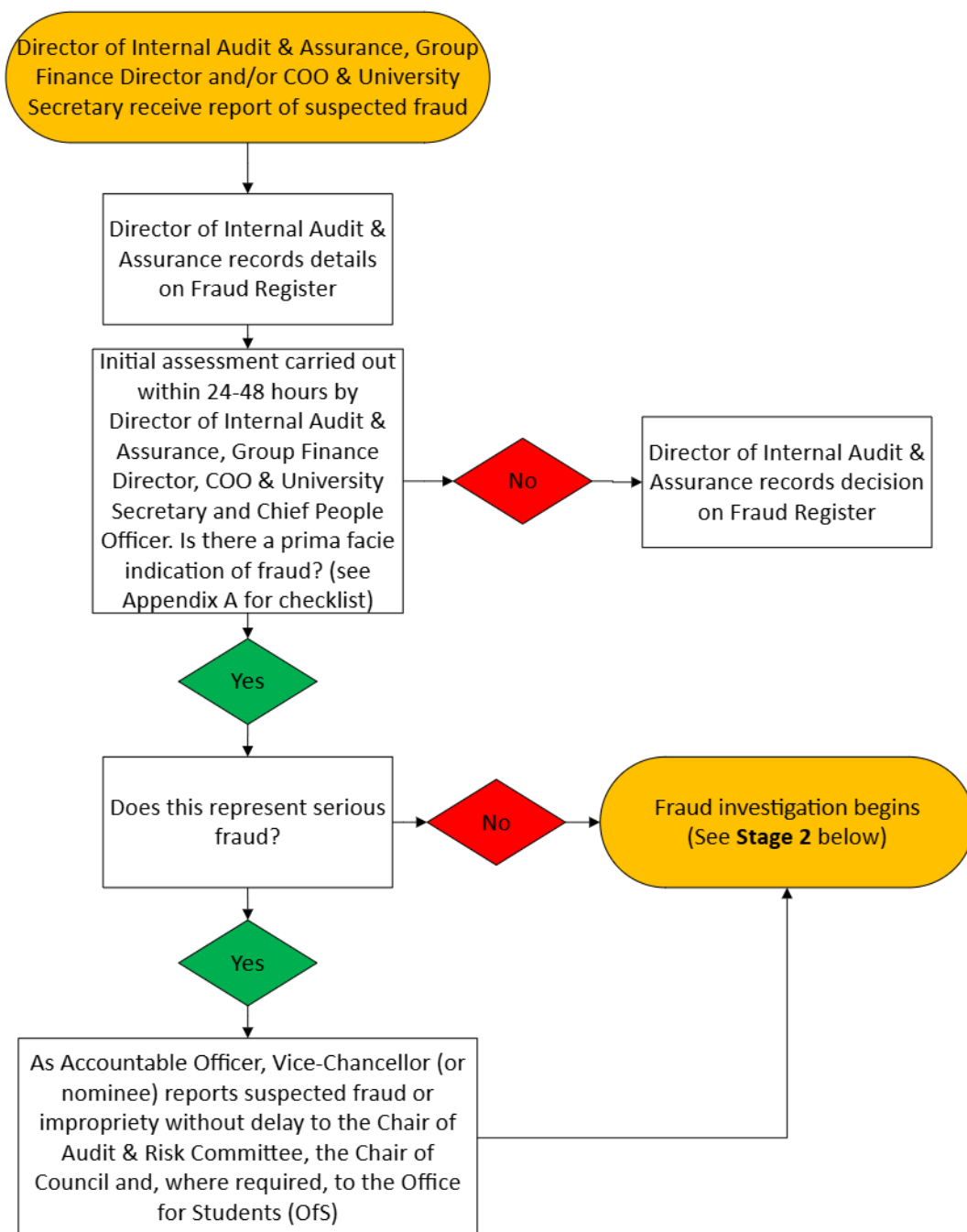
Should fraud be discovered during the course of a routine Internal Audit, the Director of Internal Audit and Assurance will inform the Chief Operating Officer & University Secretary and Group Finance Director. If fraud is discovered during an external audit, the audit sponsor should report this using one of the reporting options outlined above.

Upon receiving a report of suspected fraud, the Director of Internal Audit & Assurance, Group Finance Director and/or Chief Operating Officer & University Secretary will invoke the University's Fraud Response Plan, to ensure that suspected fraud is investigated appropriately.

Fraud Response Plan

The University’s Fraud Response Plan has three stages: Initial Assessment, Fraud Investigation, and Reporting & Acting upon the Findings of a Fraud Investigation. The University’s response to a suspected fraud may include civil recovery proceedings to recover any financial losses; referral to professional bodies; and/or reporting to the Police or other criminal investigation agencies. All suspected fraud cases are recorded on a **Fraud Register**. This document holds/tracks any actions arising from fraud investigations and is overseen by the Director of Internal Audit & Assurance, Chief Operating Officer & University Secretary and Group Finance Director.

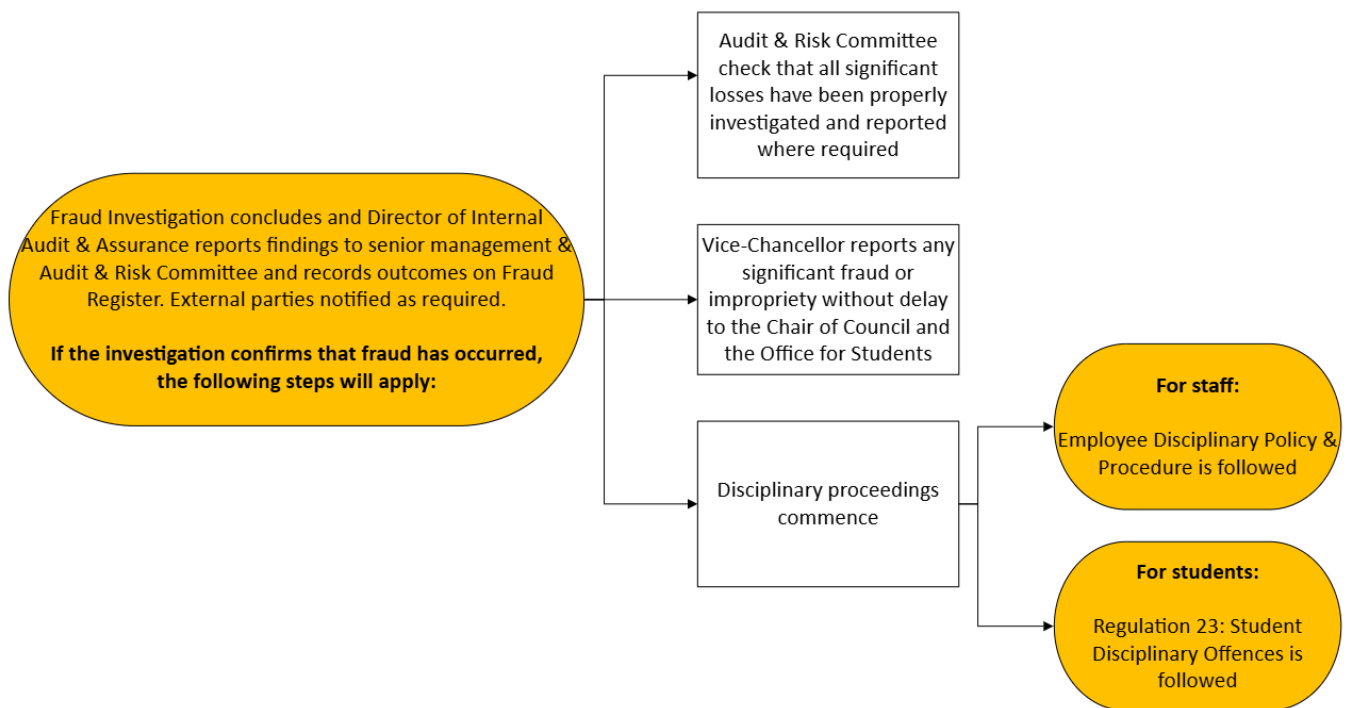
Stage 1: Initial Assessment



Stage 2: Fraud Investigation

If the Stage 1 initial assessment concludes there is a prima facie indication of fraud, a fraud investigation will commence. Relevant parties (e.g. Audit & Risk Committee, the OfS and/or funding bodies) will be notified as required that a fraud investigation is underway. Depending on the nature and severity of the suspected fraud, a fraud investigation may be carried out by Internal Audit, by the Police or by an external third party engaged by the University to undertake the investigation. Where a police investigation is initiated, the University may pause or limit internal investigative processes where necessary to avoid prejudicing any criminal investigation or subsequent proceedings.

Stage 3: Reporting and acting upon the findings of a Fraud Investigation



The report provided to Audit & Risk Committee upon completion of the fraud investigation will typically include:

- A description of the incident, including the value of any loss, the people involved and the means of perpetrating the fraud,
- Actions taken to prevent recurrence,
- A plan detailing any recommendations and actions (with timings) required to strengthen future fraud responses.

Once a fraud investigation has fully concluded and findings reported via appropriate channels, a lessons learned exercise will be carried out as referenced in the 'Continuous Improvement' section of this COP. Any recommendations arising from the Fraud Investigation report and/or lessons learned exercise will be applied to the **Fraud Register**.

Training and Communications

All Finance Office and Legal staff, Fin Regs Champions and Fraud Risk Owners must complete the [BUFDG e-learning course](#) "ECCTA - Failure to Prevent Fraud". All these staff must then repeat the course every two years as a refresher.

Beyond this, the Finance Office provides targeted training and briefing sessions on financial fraud risk, as required. Admissions staff receive training on assessing qualifications (UK and International) to mitigate the risk of identity fraud in the student application process. Regular refresher sessions and updates are provided to ensure staff remain aware of emerging risks, regulatory changes and system enhancements. This includes scenario-based learning and guidance on identifying red flags in applications. Student Recruitment Agents acting on behalf of the University are regularly trained by the Student Recruitment team through in-country visits, agent newsletters, a bi-annual conference and robust agent portal.

The University also has a **Fraud Communications Plan** in place, using defined internal communications channels to inform the wider University community how to identify and report suspected fraud.

Institutional Fraud Risk Assessment and Control Measures

The University maintains a comprehensive **Fraud Risk Assessment**, which is periodically reviewed by the Head of Risk & Resilience, together with fraud risk owners. Potential fraud risks and any associated mitigation are documented across the full remit of University activity, encompassing both financial and non-financial fraud risks. This Fraud Risk Assessment documentation is held centrally within the Risk & Resilience team in the Governance, Assurance & Risk Group (GARG), but responsibility for mitigating the individual fraud risks rests with those noted as risk owners within the University's Fraud Risk Assessment.

Where fraud risks are identified that, in line with the University's risk appetite and scoring methodology, represent a significant risk to a department, these risks should be recorded within the departmental risk register and managed by the nominated risk owner. Such risks should be monitored until mitigated to an acceptable level, and, where material to the wider institution, aligned with and reflected within the University's central Fraud Risk Assessment.

Controls in place to mitigate the University's fraud risks include:

- Directive: documented policy & process, awareness raising via internal communications plan and provision of staff training (see 'Training & Communications').
- Preventative: segregation of duties, internal checks and senior oversight, approval workflows built into systems and contract ready provisions prepared by Legal & Compliance Services. This includes a general crime compliance clause that can be inserted into relevant agreements as required (in consultation with Legal & Compliance Services), alongside optional audit rights, termination rights, subcontractor flow-down obligations, warranties, and reporting duties for higher risk contracts. A contract type risk assessment has also been completed, to identify which University templates require ECCTA clauses (such as consultancy, equipment usage, sponsorship, short courses, and international agreements) and which do not. This gives us a clear framework for when and how ECCTA provisions should be applied going forward.
- Detective: audits, monitoring systems.

- Corrective: disciplinary procedures, legal recourse, lessons learned exercises (see 'Continuous Improvement' section of this COP below).

The specific controls in place to mitigate each fraud risk are recorded within the Fraud Risk Assessment documentation, with risk owners responsible for overseeing that controls are implemented effectively to mitigate the risk.

Continuous Improvement

Following the conclusion of each fraud investigation, a lessons learned exercise will be conducted by the Internal Audit & Assurance team with relevant parties. Any recommendations arising from lessons learned exercises and/or Fraud Investigation reports will be monitored by the University Audit & Risk Committee.

An annual fraud report is submitted to the Audit & Risk Committee, providing opportunity for scrutiny and challenge. The report summarises:

- The number and nature of fraud risks recorded on the University's Fraud Risk Assessment, together with an overview of risk scores and any significant changes since the previous report.
- Progress made against any actions recorded on the University's Fraud Register.
- Summary of reported incidents, emerging trends, and actions taken.
- Any changes in legislation and the University response to those changes.

This COP will be reviewed in line with Anti-Fraud Policy review to seek feedback and ensure continuous improvement. Review of the COP will include drawing upon sector intelligence to test our approach to fraud risk assessment and controls, and to ensure we are on top of any emerging fraud-related risks.

New versions of the COP may be created before a scheduled review date due to regulatory or legislative change, end user feedback, recommendations made following a fraud investigation report and/or lessons learned exercise or due to assurance reporting generated via internal controls revealing that something is not working effectively.

The Head of Risk & Resilience & Head of Compliance & Assurance are responsible for scheduling review sessions, enacting any required changes to the COP over time, informing end-users when a new version of the COP has been issued, managing version control, archiving old versions and updating the 'live' PDF version as required.

Appendix A – Initial Assessment Checklist

When the Director of Internal Audit & Assurance, Group Finance Director, Chief Operating Officer & University Secretary and Chief People Officer convene for their initial assessment of a report of suspected fraud, they will need to determine the following:

- A. Whether further fact finding is required in order to determine the instigation of an investigation.
- B. Whether an investigation is required (prima facie indication of fraud) using checklist below and, if so, whether this represents serious fraud. Selection of any criteria applicable could indicate a need for further investigation:

1. Dishonesty

- Is there evidence the individual acted dishonestly or attempted to deceive?
- Do their actions contradict what a reasonable and honest person would consider acceptable?

2. False Representation

- Has any information been presented that is false, misleading, or incomplete?
- Was the representation made knowingly, or without belief in its truth?
- Did the representation create a false impression that influenced a decision or outcome?

3. Non-Disclosure of Material / Relevant Information

- Was relevant information withheld where there was a duty to disclose it?
- Did the omission create a misleading picture or conceal a risk, liability, or fact?
- Would a reasonable person expect the information to have been disclosed?

4. Abuse of Position

- Did the individual use their position of trust, authority, or responsibility improperly?
- Was the position used to gain an advantage or cause detriment to another party?
- Were controls bypassed or overridden without justification?

5. Fraudulent Intent

- Is there evidence the actions were taken to secure personal or institutional gain or benefit?
- Is there evidence of intent to cause loss or expose another to risk of loss?
- Do the circumstances suggest purposeful manipulation rather than error or misunderstanding?

6. Possession or Use of Fraud-Related Articles

- Has the individual possessed, created, or supplied documents, devices, or data that could facilitate fraud?

- Is there evidence of preparation or enabling activity (e.g. forged documents, altered records, access tools)?
- Were such items used or intended for use in a fraudulent act?

- C. Who should lead the investigation.
- D. Who should undertake the investigation and the composition of any project group set up to coordinate the investigation.
- E. Whether, and at what stage, Internal Audit need to be involved in the investigation - and whether a special audit is warranted.
- F. Whether the staff member or members need to be suspended, and/or have access to relevant systems suspended/ restricted.
- G. Whether the matter should be reported to the police or other enforcing authority.
- H. What stakeholder communications should be undertaken at this stage e.g. advising the Chair of the Audit & Risk Committee, Chair of the Council, and if appropriate external bodies/parties (if initial assessment indicates the case meets the criteria for this).
- I. Whether other areas need to be informed in order to comply with legal and regulatory requirements.