



**Higher Education Services
Fraud Risk Management Policy**

October 2025

DOCUMENT INFORMATION AND VERSION CONTROL

Name of policy/procedure: Higher Education Services Fraud Risk Management Policy

Document owner: Academic Registrar

Date of creation: 21st October 2025

Equality Impact Assessment date and reference 21st October 2025

Date of last review: 21st October 2025

Reviewed by: Prof. Dr Alison Watson

Date of next review: 21st October 2028

Related documents:

Version	Author	Date	Brief summary of changes
1	A. Watson	21/10/25	Original version

Contents

1.0 Introduction.....	4
2.0 Policy Statement.....	4
3.0 What is Fraud?.....	5
4.0 Relationship to the FutureLearn’s Values and Other FutureLearn Policies.....	6
5.0 Fraud Control Strategy.....	6
A. Roles and Responsibilities.....	6
(i) Board and Audit and Risk Committee.....	6
(ii) Senior Leadership Team (SLT).....	7
(iii) All Managers.....	7
(iv) People and Culture.....	7
(v) Fraud and Theft Response Team.....	7
B. Corporate Risk Register.....	8
C. Fraud Risk Assessment.....	8
D. Fraud Prevention and Detection Controls.....	9
6.0 Managing Third Party Fraud Risk.....	9
7.0 Fraud Reporting.....	10
8.0 Fraud Response Procedures.....	11
9.0 Record Keeping and Accounting.....	11
10.0 Reporting and Public Statements.....	11
11.0 Monitoring of Fraud Policy Effectiveness.....	11
12.0 Training.....	11
13.0 Policy Non-Compliance.....	11
14.0 Policy Review.....	12
Appendix.....	13
Appendix A – Definitions.....	13
Appendix B – Indicators of Fraud.....	14
Appendix C – Sample Controls.....	15

Higher Education Services Fraud Risk Management Policy

1.0 Introduction

1.1 The purpose of this policy is to support FutureLearn in effectively managing the risk associated with fraud and provide the guiding principles used to set direction on the identification, assessment, mitigation, monitoring and reporting of fraud in the company. This policy is designed to ensure compliance with the Office for Students' Condition E8 (Annex B) and all relevant regulatory requirements for higher education providers.

1.2 FutureLearn is committed to fraud prevention, detection, and deterrence and will address not just internal fraud risks (i.e. fraud perpetrated by parties within the organisation), but also external fraud risks such as fraud perpetrated on the organisation by outside parties including identity theft, ransomware, data breaches, and a wide range of corruption schemes that continue to evolve.

1.3 The organisation's activities require significant funds and the organisation is accountable to a wide range of stakeholders for the use and management of those funds. It is the responsibility of all officers and staff to ensure that FutureLearn funds and resources are used honestly and appropriately, and to report any circumstances which may indicate their improper use. This responsibility aligns with FutureLearn's value of Integrity and policies listed in section 3, and this policy builds on that value by setting out the approach and channels for reporting and managing incidents of fraud.

1.4 This policy is aligned with the Committee of Sponsoring Organisations of the Treadway Commission (COSO), Internal Control Framework and Principles on Fraud Risk Management. It also aligns to obligations placed on the University in the Financial Memorandum/ Partnership Agreement between the organisation and its funding Department, DfE/OfS.

1.5 FutureLearn is committed to ensuring that Student Loans Company funding is used solely for its intended purpose. FutureLearn will verify student identity, monitor attendance and engagement, maintain robust financial controls, and provide staff training on SLC rules and fraud risks. Any suspected misuse will be reported promptly to the SLC and relevant authorities, and student disciplinary action will be taken where appropriate. These arrangements will be reviewed regularly in line with sector guidance and regulatory expectations.

1.6 This policy will be published and made accessible to all staff, students, and relevant third parties.

2.0 Policy Statement

2.1 FutureLearn is committed to acting professionally, fairly and with integrity in all our business dealings and relationships, and to implementing and enforcing effective systems to counter fraud. As part of our zero-tolerance approach to fraud, we will not pursue, accept, or retain any business or profits that are derived from, or associated with, fraudulent or criminal conduct.

2.2 FutureLearn has a zero-tolerance approach to all forms of financial crime. Therefore, this policy establishes management's framework of internal controls for the prevention and detection of fraud and theft within the organisation, as well as protocols for conducting investigations.

2.3 This Policy applies to any attempted, suspected or actual fraudulent activities or theft involving students/learners, employees, as well as the Board/Committee Co-Optees, and third parties with a business relationship with FutureLearn.

2.4 Any employee, student or service provider may submit a report relating to potential fraud without fear of dismissal or victimisation. Investigations will be conducted without regard to the suspected employee's or third party's length of service, position/title, or relationship to the organisation. Decisions

to prosecute or refer to regulatory agencies and/or law enforcement will be made by the Fraud and Theft Response Team which comprises:

- Finance Director (Chair)
- Director of HR (Deputy Chair)
- Finance Manager
- Other co-opted individuals as deemed necessary
- Managing Director or Executive Chair

- Chair of the Audit and Risk Committee (ARC)

2.5 For cases of non-academic student fraud, following investigation and where appropriate, cases will be referred to the Student and Academic Affairs Team Director of Academic Affairs, who will determine if/when the case is referred to the Office of the Managing Director for consideration under the approved Student Conduct and Student Disciplinary procedures.

2.6 Management is expected to be familiar with the types of fraud that could occur within their specific areas of responsibility and report any suspected or known instances. Appendices outline the main types of fraud, warning signs, and controls.

2.7 Significant fraud incidents and the outcomes of fraud risk assessments will be reported to FutureLearn's OfS Accountable Officer in accordance with regulatory requirements.

3.0 What is Fraud?

3.1 Engaging in fraud is a criminal offence. Fraud is the making of dishonest statements, usually to make a gain or cause another a loss. Fraud can also involve dishonestly withholding information or dishonestly abusing a position of trust. For fraud to be committed, there does not have to be any gain or loss to another person. All that matters is that the person engaging in the fraudulent behaviour intended to cause a gain or loss.

3.2 It is also a criminal offence to dishonestly make an incorrect accounting or business record (this is often referred to as false accounting) or to dishonestly evade tax or otherwise cheat the tax authorities (tax fraud).

3.3 Fraud can take many forms:

- **Fraud by false representation:** It is a fraud if a person dishonestly makes a false representation and, in doing so, intends to make a gain for themselves, FutureLearn, or one of FutureLearn's customers, or to cause a loss to another person. A representation is false if it is untrue or misleading and the person making it knows that it is, or might be, untrue or misleading.
- **Fraud by omission:** It is a fraud if a person dishonestly fails to disclose to another person information which s/he is under a legal duty to disclose and, in doing so intends to make a gain for themselves, FutureLearn, or one of FutureLearn's customers, or to cause a loss to another person. Remaining silent when you have an obligation to inform another person of something is just as much of a fraud as providing a person with false information.
- **Fraud by abuse of position:** It is a fraud if a person occupies a position of trust and dishonestly abuses that position and, in doing so, intends to make a gain for themselves, FutureLearn, or one of FutureLearn's customers, or to cause a loss to another person.
- **False accounting:** It is fraud for a person to dishonestly destroy, conceal or falsify any account, record or document made or required for any accounting purpose and, in doing so, intends to make a gain for themselves, or someone else, or to cause a loss to another person. False accounting could involve dishonestly altering financial records, recognising revenue or costs in the wrong financial year, moving costs between projects, or failing to disclose documents to auditors. Purely internal false accounting could still amount to fraud even where there is no gain or loss to FutureLearn or a third party.

3.4 There does not have to be a financial gain or loss for fraud to have occurred. Fraud can be non-financial. Examples of non-financial fraud include: deliberately overstating environmental or diversity statistics or credentials, deliberately overstating capabilities in bids or tenders, making false or misleading statements to regulators or insurers, misrepresenting project performance, or making false statements in advertising or marketing materials.

3.5 If one of the FutureLearn's employees, agents or third party service providers were to engage in fraudulent conduct and in doing so intended to benefit FutureLearn or one of FutureLearn's customers, then FutureLearn could face criminal liability for failing to prevent that person from engaging fraud.

3.6 FutureLearn has put in place and will maintain reasonable procedures designed to prevent its employees, agents or third party service providers from engaging in fraud. These policies and procedures are designed to meet the standards of the guidance issued by the UK's Home Office under the Economic Crime and Corporate Transparency Act 2023.

4.0 Relationship to the FutureLearn's Values and Other FutureLearn Policies

4.1 The Board and Management have adopted this Fraud Risk Management Policy as a complement to the FutureLearn's policies designed to foster and promote the highest standards of ethical practices across the organisation. Employees at every level have responsibility for ensuring that the organisation's activities align with FutureLearn's Values as well as other policies designed to ensure compliance with laws, rules, and regulations in the jurisdictions in which the organisation operates. These include the following:

- [Anti-Bribery and Corruption Policy](#)
- [Staff Disciplinary Procedure](#)
- [Research & Ethics Policy](#)
- [Gifts, Gratuities and Hospitality Policy](#)
- [Purchase Card Policy](#)
- [Staff Whistleblowing Policy](#)
- [Student Whistleblowing Policy](#)
- [Code of Conduct](#)
- [Travel and Expenditure Policy](#)
- [Conflict of Interest Policy](#)

5.0 Fraud Control Strategy

A. Roles and Responsibilities

5.1 All FutureLearn staff, regardless of their level, are responsible for helping deter and defend the organisation from fraud and theft. The section below highlights the roles and responsibilities within the FutureLearn's Fraud Risk Management Framework.

(i) Board and Audit and Risk Committee

5.1.2 To set the appropriate tone for the organisation, the Board is responsible for ensuring that management designs an effective Fraud Risk Management Framework. The Board has delegated this responsibility to the Audit and Risk Committee. The Audit and Risk Committee should:

- Periodically review and approve FutureLearn's Fraud Risk Management Policy, as well as other applicable policies and procedures designed to help mitigate fraud risk.
- Receive assurances from the External Auditor and Internal Audit regarding assessment of the risk of fraud by management, including the risk of management's override of controls, and ensuring that controls are designed and functioning to deter, prevent, and detect fraud by management.

- Be fully informed about instances of fraud that occur within the organisation involving senior-level employees or employees about whom significant internal control issues are uncovered, together with progress on the related investigation and lessons learned.
- Ensure that the Internal and External Auditors, and appropriate authorities, have been informed of cases where appropriate.

(ii) Senior Leadership Team (SLT)

5.1.3 Management has overall responsibility for the design and implementation of the FutureLearn's Fraud Risk Management Framework, including:

- Ensuring that fraud is addressed in FutureLearn's strategic objectives and risk assessment activities.
- Appointing the fraud control officer, who has overall responsibility for the coordination and implementation of the FutureLearn's Fraud Risk Management Framework as well as reporting to the Audit and Risk Committee about fraud risk matters.
- Identifying and assigning staff responsible for anti-fraud control activities, as outlined in the fraud risk register and associated mitigation plans, and maintaining records that verify that those processes and controls have been properly executed.
- Providing defined, proactive processes and control activities to deter, prevent, and detect fraud.
- Implementing internal controls designed to prevent and/or detect fraud within each department and faculty.
- Promote understanding of, training on, and compliance with this Fraud Risk Management Policy, and other related corporate policies listed in section 3 above.
- Maintaining an open-door policy and other mechanisms to report fraud and misconduct.

(iii) All Managers

- **5.1.4** Ensuring fraud control activities, both preventative and detective, are identified, developed, implemented and monitored.
- Facilitating new employee orientation and other employee training activities.
- Escalating issues involving potential fraud reported by management and employees.
- Participating in management's fraud risk assessment activities.

(iv) People and Culture

5.1.5 The HR Director (GUS) assists management and employees by supporting key anti-fraud control activities including:

- Supporting internal fraud investigation activities, as needed.
- Coordinating disciplinary or corrective action, if deemed necessary by the Fraud and Theft Response Team.
- Providing access to and monitoring of training via the Learning Management System.

(v) Fraud and Theft Response Team

5.1.6 If a fraud incident has occurred or a suspicion that fraud has taken place is raised then, and as soon as practicable, a meeting of the Fraud and Theft Response Team should be convened to decide on the path of action.

5.1.7 The Fraud and Theft Response Team will consist of the Finance Director, Managing Director, Chief Operating Officer, Legal Counsel and the Director of HR, and report into the Board and Audit and Risk Committee.

5.1.8 This team will:

- Be responsible for taking forward FutureLearn's response to any potential fraud incident.
- Consider the information available (via the Fraud Notification Form if one has been submitted).
- Decide:
 - Whether an investigation is required.
 - If so, commission the investigation, determine who should undertake it, and the composition of any project group set up to co-ordinate it. (Where this relates to a member staff, the investigation will be conducted in line with the provisions of the staff Disciplinary Procedures).
 - Whether external legal advice or support with the investigation is required.
 - Whether, and at what stage, Internal Audit need to be involved in the investigation.
 - Whether FutureLearn's insurers need to be informed.
 - Whether the staff member(s) or student(s) need to be suspended.
- **5.1.9** Following the completion of any investigation:
 - Consider the corporate reporting responsibilities including:
 - Whether the matter should be reported to the police.
 - What stakeholder communications should be undertaken at this stage e.g. including notifying the Managing Director, Internal and External Auditors, Chairs of Board and ARC, and Office for Students.
 - Consider what remedial steps, if any, need to be taken.
 - Consider whether the matter needs to be referred to FutureLearn's HR department.
 - Consider whether external legal advice is required.

B. Corporate Risk Register

5.2 FutureLearn's Corporate Risk Register is administered by the Finance Director who reports to the Audit and Risk Committee on risk matters, including fraud risk. The Audit and Risk Committee will provide an annual assurance statement to the Board and OfS Accountable Officer confirming the adequacy and effectiveness of fraud risk management arrangements.

C. Fraud Risk Assessment

5.3 FutureLearn is committed to the timely prevention and detection of fraud and theft and is mindful of the UK Government's Framework to prevent Fraud Offence. The external auditors conduct an annual fraud risk assessment to identify, assess, and respond to key fraud risks in the organisation. Evidence of this self-assessment must be recorded in a fraud risk register with a description of the risk and associated control(s) mitigating the risk identified.

5.3.2 The fraud risk assessment process considers key factors that drive fraud such as opportunities, incentives and pressures, and attitudes and rationalisation. The risk assessment methodology consists of:

- identifying business unit and process-level fraud risks using common fraud scenarios;
- prioritising the likelihood and impact of such risks on an inherent and residual basis through review by the Audit and Risk Committee;
- mapping fraud risks to internal controls;
- and identifying potential gaps or enhancement opportunities related to management's anti-fraud control activities.

5.3.3 The results of management's fraud risk assessment are addressed within an action plan and shared with the Audit and Risk Committee. Recommendations arising from audits will be tracked and implemented, with progress reported to the Audit and Risk Committee

5.3.4 The output from the fraud risk assessment informs FutureLearn's approach to managing its fraud risk through this policy and other fraud prevention and detection measures.

D. Fraud Prevention and Detection Controls

5.4 FutureLearn has designed a combination of preventive and detective anti-fraud control activities which occur at various levels of the organisation and are intended to help mitigate the occurrence of fraud and theft as well as ensure the timely detection of fraud risk events within operations.

5.4.2 FutureLearn's high-level fraud prevention control activities include:

- Human resource procedures such as selected pre-employee background checks, training, employee surveys, and exit interviews.
- Physical access control activities address admittance to organisations facilities and right to use of assets, such as inventory.
- Logical access control activities address access rights to sensitive information.
- Transaction control activities address procurement procedures and managerial approval requirements.
- Separation of duties to ensure that key functions and controls are not performed by the same person.
- Adequate supervision and workload management.
- Technological control activities include electronic third-party screening activities and automated restrictions on certain payments that present elevated risk to the organisation or do not comply with prescribed FutureLearn policy requirements.

5.4.3 FutureLearn's high-level fraud detection control activities include:

- Data analytics utilised by the Finance directorate to continuously monitor certain types of payments and transactions, as well as data analytics used by the internal audit function in its performance of operational audits (as relevant).
- Reporting mechanisms to receive, retain, and treat concerns, complaints, and information about potential violations of fraud across the FutureLearn operations.
- Line management review and approval of staff activity including but not limited to spend requests, reports, etc.
- Periodic reconciliations of accounts.
- Random spot checks.
- Complete and secure audit trails.
- Appropriate performance monitoring.
- Frequent budgetary and other financial reviews/reports.

6.0 Managing Third Party Fraud Risk

6.1 As per FutureLearn's Higher Education Services Academic Partnerships & Due Diligence Policy, third parties who provide services for and on behalf of FutureLearn are subject to risk-based due diligence to ensure their suitability as a business partner of FutureLearn can be assessed.

6.2 All contracts with third parties who provide services for and on behalf of FutureLearn should be in writing and contain appropriate anti-financial crime wording.

6.3 No payments can be made to any third party unless an approved contract is in place.

6.4 All contracts and engagements with third parties who provide service for and on behalf of FutureLearn are subject to a programme of monitoring and review on a periodic basis to ensure compliance with this Policy.

6.5 Services provided and payments made to and by third parties who provide service for and on behalf of FutureLearn should be monitored. Any receipt or invoice should be provided by the third party, which should set out in reasonable detail the goods, services or expenses for which payment is requested. All receipts and invoices should be scrutinised by the person who receives the receipt or invoice and by the person who approves the payment.

6.6 Students may also be the perpetrators of fraudulent activity including accessing tuition fee and maintenance loan finance from the Student Loans Company ("SLC"). FutureLearn takes active steps to prevent and detect student fraud in accessing SLC funding to help safeguard public funds and maintain compliance with regulatory expectations including the following measures:

- **Identity checks** are carried out for all students on enrolment.
- **Attendance and engagement** by students are monitored, with prompt reporting of non-engagement or withdrawal to the SLC to prevent continued payments to ineligible students.
- **Regular audits and reconciliations** help identify anomalies in SLC funding receipts.
- **Staff training** ensures awareness of SLC rules and fraud risks including the provision of guidance on recognising red flags, such as suspicious documentation or unusual enrolment patterns.
- **Collaboration** with the SLC and sector partners to share intelligence on fraud risks and emerging trends.
- **Controls and procedures** reviewed regularly to ensure they remain effective and in line with sector best practice.
- **Suspected misuse** is escalated to the Audit and Risk Committee and reported to the SLC as required.

7.0 Fraud Reporting

7.1 All attempted, suspected or actual incidents should be reported immediately either:

- To the Head of Department and/or the Chief Strategy & Finance Officer. The Head of Department should then inform the Chief Strategy & Finance Officer or, in their absence, the Chief People Officer.
- Anonymously via the Reporting a Fraud form.
- Via the FutureLearn Raising Concerns (Whistleblowing) Policy; provided reports are made in good faith then an individual is protected by the FutureLearn against harassment or victimisation and the individual's confidentiality must be preserved. The Chief Operating Officer, on receiving notifications allegedly related to fraud, will inform the Chair of the Fraud and Theft Response Team. The Team will determine if the matter should progress through the Fraud and Theft Response route or the Whistleblowing route.
- By sending an email to fraud@futurelearn.com.

7.2 If the disclosure involves or implicates any of the individuals identified above, then the disclosure should be made to the Chair of the Board and/or the Chair of Audit & Risk Committee as appropriate.

7.3 On being alerted to circumstances which give rise to suspicion of fraud or theft, the Finance Director, under the instruction of the Managing Director will convene a meeting of the Fraud and Theft Response Team (and Head of Department if deemed necessary) who will then review the preliminary findings and, where appropriate, in conjunction with the Chief People Officer decide whether to:

- Discontinue the investigation if initial suspicions are not confirmed, or
- Continue with a full internal investigation.
- Engage the assistance of Internal Audit.

7.4 Third parties are encouraged to report fraud impacting the organisation either through the Whistleblowing Policy or by sending an email to fraud@futurelearn.com.

8.0 Fraud Response Procedures

8.1 FutureLearn's Fraud and Theft Response Procedure outlines the process to be adopted if attempted, suspected or actual fraud is reported or detected and clearly defines the authority levels, responsibilities for action and reporting lines.

9.0 Record Keeping and Accounting

9.1 Books, records and accounts must be kept which accurately and fairly reflect all transactions.

9.2 FutureLearn takes steps to ensure that (i) financial records are not altered dishonestly, (ii) revenue is recognised in accordance with generally accepted accounting practices, (iii) costs are accurately recorded to the correct project, and (iv) documents will be retained for appropriate periods of time.

9.3 FutureLearn will ensure that its Annual Financial Return and all other data submitted to the Office for Students (including data relating to the use of public funds) is accurate.

9.4 FutureLearn will not conceal or fail to disclose documents to its auditors.

10.0 Reporting and Public Statements

10.1 FutureLearn's annual report, financial statements and other public statements must be accurate. This includes any environmental, diversity and inclusion, or any other environmental, social or governance reporting.

10.2 FutureLearn must be honest and accurate in all its dealings with regulators or other government bodies.

11.0 Monitoring of Fraud Policy Effectiveness

11.1 The design of the components within the Fraud Risk Management Framework will be evaluated during management's annual fraud risk assessment, or sooner, should a fraud risk event occur. The operating effectiveness of related anti-fraud controls will be tested periodically by Internal Audit.

11.2 Periodically, the internal audit function may conduct a separate and independent evaluation of the Fraud Risk Management Framework utilising authoritative guidance and leading practices. Internal Audit will report its findings to the Audit and Risk Committee and senior management. The fraud control officer is responsible for ensuring that any deficiencies, weaknesses, or enhancements involving anti-fraud controls are addressed in a timely and effective manner. In addition, internal audits will consider the risk of fraud as part of its operational audits conducted throughout the course of the year.

12.0 Training

12.1 Training on Fraud Awareness should be completed by all staff on the Learning Management System and refreshed every two years.

12.2 Targeted technical training should be provided on the fraud risk management process e.g., training on conducting risk identification, assessment and the documenting risks and controls on the fraud risk register. Senior Managers are responsible for ensuring that the right staff members are identified to attend the training session.

13.0 Policy Non-Compliance

13.1 If non-compliance with this policy is identified, the policy owner and/or the Fraud and Theft Response Team must assess the impact of the non-compliance and document, as appropriate, the

planned remediation. Any instances of policy non-compliance must be logged on the fraud risk register with a corresponding action plan detailing the planned remediation.

14.0 Policy Review

14.1 This Policy will be assessed by management and reviewed by the FutureLearn's Audit and Risk Committee every three years. Any changes to the Policy will be communicated to organisation staff and relevant third parties in a timely manner.

Appendix

Appendix A – Definitions

1. **Corruption:** Misuse of entrusted power for private gain, including bribery or favouritism.
2. **Fraud:** Wrongful or criminal deception intended to result in financial or personal gain.
3. **Theft:** Theft is defined under the Theft Act 1968 as “Dishonestly appropriating the property of another with the intention of permanently depriving them of it, immaterial of whether the appropriation is made with a view to gain. This may include the removal or misuse of funds, assets or cash.”
4. **Whistleblowing:** The reporting of wrongdoing or risk internally or externally in good faith.

Appendix B – Indicators of Fraud

Do individuals appear to live an expensive lifestyle that seems disproportionate to their means?

Do individuals seek to override standard procedures without justification?

Are there people who are reluctant to take annual leave or are overly secretive about their work?

Are there related party transactions (i.e. business activities with personal friends, relatives or their companies)?

Are there unrecorded or unmanaged conflicts of interest?

Are people subject to unachievable or unrealistic deadlines or targets?

Is there inadequate or inappropriate segregation of duties regarding initiation, authorisation and recording of transactions, maintaining custody of assets and the like?

Are there transactions that receive minimal oversight or where one person seeks to manage the whole transaction without input from others?

Are documents missing, copies rather than originals, in pencil or altered, or do they contain false signatures, the signature of an incorrect person or no authorisation where it would be expected?

Is there deviation from standard procedures (for example, all files but one having been handled a particular way or all documents but one having been included in a file)?

Are there excessive or poorly evidenced journal entries, or a lack of explanation for journal entries?

Is there a request to move costs from one project to another?

Are materials, goods or services fictitiously or erroneously reported as having been purchased, with evidence fabricated to support the claim, so they can be used as a conduit to remove funds from the organisation? Potential evidence could include:

- repeated purchases of the same items;
- identical items purchased in different quantities within a short time period;
- invoices and statements used as evidence for purchases facilitating duplicate transactions or payments;
- anomalies in the format of purchase invoices; or
- goods and equipment not being used as promised, or that do not work or do not exist.

Service providers not providing evidence to support their charges or sums claimed for.

Appendix C – Sample Controls

1. Background checks during hiring and exit interviews.
2. Mandatory holidays and job rotation.
3. Regular reconciliation and independent audit checks.
4. Segregation of duties across key financial processes.
5. Whistleblower protection and confidential reporting routes.