Anti-Fraud and Anti-Corruption Policy

Version 1.0

Purpose:	This policy sets out the responsibilities of the Institute, its employees, students and those working on behalf of the Institute in observing and upholding the Institute's commitment to preventing fraud, bribery, corruption and deliberate financial misconduct.
Circulation:	This document is available for all to review and will be published on the Institute's website
Policy author:	Vice President for Finance and Corporate Affairs
Policy Owner:	Audit, Risk and Compliance Committee Governing Body
Approval:	Executive Board Audit, Risk and Compliance Committee
Approval Date:	Governing Body 14 July 2026

Internal Use Only

Revision History

Version no.	Date	Classification	Owner	Summary of Changes
V1.0	06 July 2026	Public	VP for Finance and Corporate Affairs	Initial Draft

Approval

This document requires the following approvals:

Name	Approval Date
Executive Board	06 July 2026
Audit, Risk and Compliance Committee	09 July 2026
Governing Body	14 July 2026

Date of Next Review	July 2028

Table of Contents

DkIT Anti-Fraud and Anti-Corruption Policy

1. Introduction

Dundalk Institute of Technology (DkIT / the Institute) is committed to preserving the highest standards of honesty, transparency, probity, accountability and ethical conduct in all of its activities. Wrongdoing such as bribery, fraud, corruption or malpractice, or the covering up of these, can have a devastating effect on professional reputations, working relationships and morale. Often, staff or students can be the first to know when someone inside or connected with the Institute is involved in illegal or improper activity and practices, but often they feel apprehensive about reporting their concerns.

This Policy applies to fraud and corruption committed through physical, electronic, digital or cyber means and includes cyber-enabled financial crime, information system abuse, identity theft, data manipulation and the fraudulent use of Institute information assets.

The Institute adopts a zero-tolerance approach to fraud, bribery, corruption and deliberate financial misconduct.

2. Purpose

This policy sets out the responsibilities of the Institute, its Governing Body, employees, students, and those working on behalf of the Institute in observing and upholding the Institute's commitment to preventing fraud, bribery, corruption and deliberate financial misconduct.

The purpose of this Policy is to:

- Provide information and guidance to staff, students, contractors and others engaged in Institute activities on how to address suspicions of corrupt or fraudulent activities
- Protect public funds, Institute assets, information and reputational integrity.
- Support compliance with legislative, regulatory and governance obligations.
- Promote a culture of honesty, integrity, transparency, accountability and responsible stewardship through outlining the key principles regarding corruption, fraud prevention and detection.
- Establish arrangements for reporting, investigating and managing allegations of fraud and corruption.

3. Scope

This Policy relates to all units of the Institute, both academic and support, including its research centres and its wholly owned subsidiary companies. It encompasses all activities undertaken on Institute-owned or managed property, off-campus locations, remotely, electronically, or through third-party systems where DkIT assets, funding, information, services, or operations are involved. This Policy applies to:

- Members of the Governing Body and Governing Body Committees.
- Employees.
- Agency and temporary workers.

- Students.
- Researchers and research partners.
- Contractors, consultants and service providers.
- Any person acting on behalf of DkIT or its subsidiary companies.

4. Definitions

Fraud

Fraud means any intentional act or omission involving deception, bribery, forgery, extortion, theft, conspiracy, embezzlement, misappropriation, false accounting, collusion, concealment of material facts or false representation, undertaken to obtain an unauthorised benefit, avoid an obligation or cause loss to another party. For the purposes of this Policy, fraud includes attempted fraud.

Corruption

Corruption means the abuse of entrusted power, position or authority for private gain, including bribery, the improper offering, giving, soliciting or acceptance of an advantage, abuse of position, misuse of authority, and the improper management or concealment of conflicts of interest.

Financial Irregularity

Financial irregularity means any actual or suspected breach of financial procedures, internal controls or governance requirements that may expose the Institute to financial loss, misuse of public funds or assets, or reputational damage.

Cyber-Enabled Fraud

Cyber-enabled fraud means any fraudulent activity that uses information systems, digital communications, computer networks, electronic records or technology to obtain financial gain, an unauthorised advantage or cause loss to the Institute or another party.

It is not possible to provide an exhaustive list of activities that constitute fraud. Examples include:

- Falsifying, altering or concealing financial, administrative or other Institute records or documents.
- Submitting false or misleading claims for salaries, expenses, goods or services.
- Theft, misappropriation or unauthorised use of Institute funds, assets or property.
- Bribery, corruption, conflicts of interest or the improper offering or acceptance of gifts or hospitality.
- Procurement and purchasing fraud, including supplier payment diversion and electronic procurement fraud.
- Payroll and identity fraud, including payroll redirection and impersonation scams.
- Cyber-enabled fraud, including phishing, social engineering, credential theft, unauthorised system access and misuse of Institute systems.
- Research-related fraud, including the manipulation or falsification of research data and funds.

- Any other dishonest or deceptive act intended to obtain an unauthorised benefit or cause loss to the Institute or another party.

5. Policy Statement

DkIT adopts a zero-tolerance approach to fraud, bribery, corruption and deliberate financial misconduct.

All members of the Institute, its Governing Body, employees, students, and those working on behalf of the Institute and its subsidiary companies are expected to:

- Act honestly and with integrity.
- Safeguard Institute resources.
- Comply with applicable policies and procedures.
- Report suspected wrongdoing promptly.
- Co-operate with investigations.

Allegations of fraud, bribery, corruption or deliberate financial misconduct shall be assessed and investigated proportionately and independently and may result in disciplinary, civil or criminal action where appropriate.

The Institute ensures compliance with all mandatory reporting requirements under relevant legislation and the Institute's Code of Governance, including its obligations under the Criminal Justice Act 2011, where applicable, to report information relating to certain fraud and other specified offences to An Garda Síochána.

6. Roles and Responsibilities

Responsible Person / Group	Role
Governing Body	• Review and approve this Policy. • Adhere to the Policy Statement within this document. • Provide oversight of fraud and corruption risk. • Receive assurance regarding the effectiveness of internal controls. • Review significant incidents and associated actions.
Audit, Risk and Compliance Committee	• Review and recommending approval of this Policy to Governing Body. • Oversight of fraud risk management arrangements. • Review significant investigations. • Monitor implementation of recommendations. • Receive fraud assurance reports.
President and Executive Board	• Promote a culture of integrity and accountability. • Ensure institutional awareness and implementation of this Policy. • Escalate significant matters as appropriate.

Responsible Person / Group	Role
Vice President for Finance and Corporate Affairs	• Executive ownership of this Policy. • Co-ordination of fraud investigations. • Fraud reporting and record management. • Liaison with auditors, insurers and external authorities. • Oversight of cyber-enabled fraud risks with financial, governance or operational implications. • Co-ordination with Computer Services during investigations involving cyber incidents. • Ensure lessons learned are incorporated into control improvements.
Computer Services	• Maintain technical controls to prevent and detect cyber-enabled fraud. • Monitor suspicious activity within Institute systems. • Maintain audit logs and system records. • Support investigations involving electronic evidence. • Escalate suspected cyber-fraud incidents. • Support recovery activities following cyber incidents. • Maintain access-control and authentication standards.
Data Protection Office	• Support investigations involving breaches of personal data. • Report personal data breaches to the Data Protection Commission (DPC), where there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed', where the breach presents a risk to the affected individuals. • Monitor and advise on compliance in relation to the protection of personal data.
Heads of School/ Departments, Functional Managers, System Owners and Administrators	• Ensure appropriate access controls are maintained. • Review user permissions periodically. • Protect sensitive financial and personal information. • Report suspected cyber incidents promptly.
Employees, Students, Contractors and Others engaged in Institute activities	• Conduct Institute business honestly and ethically. • Adhere to the Policy Statement within this document. • Remain vigilant to indicators of fraud and corruption. • Complete required training. • Report concerns promptly. • Co-operate with investigations.

7. Reporting Procedures

These reporting procedures apply to all members of the Institute, including staff, students, agency staff, contractors, consultants, service providers and any third parties acting on behalf of or engaged with the Institute or its subsidiary companies. Any such person may report actual or suspected fraud, bribery, corruption, financial irregularity or unethical conduct under this Policy. All such matters should be reported promptly.

Persons making reports in good faith shall be protected in accordance with the Protected Disclosures Policy and applicable legislation.

7.1 Reporting concerns internally

Members of staff and students shall report any actual or suspected fraud, irregularity, or unethical conduct to their Head of School/Unit, immediate supervisor or relevant designated contact without delay. The person receiving the report shall notify the President or the President's nominee promptly.

7.2 Alternative reporting route

Where it is not possible or appropriate to report the matter to the Head of School/Unit, immediate supervisor or designated contact, the matter shall be reported directly to the President or the President's nominee.

7.3 Escalation where necessary

Where it is not possible or appropriate to report the matter to the President or the President's nominee, the matter may be reported to the Chair of the Audit, Risk and Compliance Committee or the Chair of the Governing Body.

7.4 Reporting by contractors and third parties

Contractors, consultants, suppliers and other third parties engaged by the Institute or its subsidiary companies are required to report any suspected fraud, bribery, corruption, deliberate financial misconduct or irregularity relating to Institute business to the relevant contract manager or designated Institute contact. Such reports may also be made directly to the President or the President's nominee where appropriate.

7.5 Protected disclosures

Nothing in this Policy prevents a member of staff, student or third party from making a protected disclosure under the Protected Disclosures Act 2014–2022. Such disclosures may be made directly under the Institute's Protected Disclosures Policy at any time.

7.6 Good faith reporting

Reports should be made in good faith and based on reasonable belief. The person reporting should take care to avoid making unfounded allegations or alerting suspected individuals. The good name and reputation of individuals will be respected in accordance with fair procedures.

7.7 Protection from penalisation

The Institute will not tolerate retaliation or penalisation against any person (including staff, students, contractors or third parties) who reports a concern in good faith.

7.8 Anonymous disclosures

The Institute does not encourage anonymous reporting; however, anonymous disclosures may be considered at the discretion of the President or the President's nominee. In determining whether to investigate, regard will be had to:

- the seriousness of the allegation;
- the credibility and specificity of the information;
- the ability to investigate and corroborate the matter;
- fairness to any person(s) named.

8. Investigation of Allegations

All reports shall be assessed and investigated in a manner that is fair, objective and proportionate.

8.1 Initial assessment (triage stage)

All reports shall be subject to an initial assessment by the President or the President's nominee to determine:

- whether a formal investigation is required;
- whether interim protective measures are necessary;
- whether referred should be made to Internal Audit, external investigators or An Garda Síochána.
- Where there has been a breach of personal data, notify the data protection office.

This process applies irrespective of whether the matter involves staff, students, contractors, third parties or any other persons acting on behalf of the Institute.

8.2 Establishment of investigation team

Where a formal investigation is required, the President or nominee shall appoint an investigation team. The team may include internal staff, Internal Audit, external specialists, forensic experts, and/or legal advisers as appropriate.

Where potential conflicts of interest arise, the investigation shall be assigned to independent personnel or external parties.

8.3 Digital evidence preservation

Investigations involving digital evidence shall be conducted in conjunction with Computer Services and, where appropriate, external forensic specialists. Where fraud involves electronic systems, DkIT shall:

- Preserve system logs.
- Preserve email records.
- Preserve network activity records.
- Preserve device and server evidence.
- Restrict access where necessary.
- Follow established digital forensic procedures.

8.4 Conduct of investigation

Investigations shall be conducted in accordance with:

- fair procedures

- natural justice
- confidentiality on a need-to-know basis
- relevant Institute policies and procedures

Any person against whom an allegation is made shall be informed of the substance of the allegation and given a reasonable opportunity to respond. This includes staff, students, contractors, consultants, third parties and any other persons acting on behalf of the Institute where applicable.

8.5 Reporting of findings

On completion of the investigation, the investigation team shall prepare a written report for the President or the President's nominee, setting out findings, conclusions and recommended actions.

8.6 Governance oversight

The President or nominee shall report significant matters, emerging trends and high-risk cases to the Audit, Risk and Compliance Committee. Where such matters have, or are likely to have, a financial impact that, in the opinion of the President, warrants the attention of the Finance Committee, they shall also be reported to that Committee.

The Audit, Risk and Compliance Committee shall provide appropriate updates to the Governing Body, including matters arising from protected disclosures, in accordance with the Protected Disclosures Policy.

8.7 External reporting obligations

Where required, the Institute shall report matters to external bodies including (but not limited to):

- Department of Further and Higher Education, Research, Innovation and Science
- Higher Education Authority (HEA)
- Comptroller and Auditor General
- Other funding or regulatory bodies
- An Garda Síochána
- Data Protection Commission
- Other statutory authorities, as appropriate

9. Training and Awareness

DkIT shall provide appropriate fraud and corruption awareness training encompassing:

- Fraud awareness.
- Cyber-fraud awareness.
- Phishing and social engineering risks.
- Procurement fraud indicators.
- Payroll diversion scams.
- Data protection obligations.
- Reporting mechanisms and responsibilities.

10. Monitoring, Reporting and Assurance

An annual Fraud Assurance Report is required by the Department of Further and Higher Education, Research, Innovation and Science to assist in their reporting requirements to the Comptroller and

Auditor General for fraud/ suspected fraud/ irregularities/ overpayments in the higher education sector. This report shall be presented to:

- Audit, Risk and Compliance Committee.
- Finance Committee (financial impacts).
- Governing Body.

The report entails disclosure as to:

- Allegations received.
- Investigations completed.
- Confirmed incidents.
- Financial impacts.
- Recoveries achieved.
- Control weaknesses identified.
- Corrective actions implemented.
- Confirmation if the case has been notified to the Higher Education Authority (HEA) and/or Comptroller and Auditor General.

A dedicated section should report on:

- Cyber-enabled fraud incidents.
- Attempted cyber-fraud attacks.
- Financial losses avoided.
- Lessons learned.
- Control improvements.
- Staff awareness statistics.
- Emerging cyber-fraud trends.

11. Confidentiality

The Institute shall treat all reports or allegations of suspected fraud, bribery, corruption or deliberate financial misconduct with appropriate confidentiality and shall handle information on a need-to-know basis to protect the integrity of any assessment or investigation and the rights of all parties concerned.

Information relating to a report shall be disclosed only to those persons who require it for the purposes of assessing, investigating or responding to the matter, or where disclosure is required by law or is necessary to protect the interests of the Institute.

All persons involved in the reporting, assessment and investigation of suspected fraud, bribery or corruption shall maintain appropriate confidentiality and comply with applicable legal, regulatory and data protection requirements. The Institute cannot guarantee absolute confidentiality where disclosure is required to facilitate an investigation, disciplinary process, legal proceedings or reporting to external authorities.

12. Related Policies and Legislative Context

This Policy should be read in conjunction with Institute's Governance Framework at Governance and Compliance | DkIT. The following policies form the core governance framework supporting fraud prevention.

- Code of Conduct

- Protected Disclosures Policy
- Conflict of Interest Policy
- Ethics in Public Office
- Data Protection Policy
- Risk Management Policy
- Disciplinary Procedure
- Procurement Policy and Procedures
- Financial Regulations
- Information Security Policy
- Gifts and Hospitality Policy (or Anti-Bribery Policy if separate)
- Acceptable Usage Policy for the users of the Institute's Computing & Network Resources
- Research Integrity Policy
- Clean Desk Policy
- Data Governance Policy
- IT Physical Security Access Policy
- Privileged User Policy
- Third Party Access Policy (Outsourcing_3rd Party Access Policy)
- Joiners Movers & Leavers User Administration Procedures for DkIT ICT Services
- AI Policy
- IT Asset Management Policy
- Personal Data Security Breach Management Procedures
- Cyber Resilience Framework

Where a matter involves both a cyber incident and suspected fraud, it shall be managed under both the relevant Information Security procedures and this Policy.