

IADT

Prevention and Detection of Fraud Policy

Document Reference and Version No	Fraud Policy Version 1.1
Purpose	Prevention and Detection of Fraud
Commencement Date	June 2020
Date of Next Review	June 2023
Who needs to know about this document	All Staff Members, All Students, All Contractors
Revision History	Version 1 Approved by Governing Body January 2015 Version 1.1 Approved by Governing Body May 2020
Policy Author	Secretary/Financial Controller
Policy Owner	Secretary/Financial Controller

IADT

Prevention and Detection of Fraud Policy

1. Introduction

1.1. Purpose

IADT recognises the importance of protecting the institute, its reputation and its employees from the consequences of fraudulent activity. Accordingly, IADT expects the highest standards of ethical behaviour from all Institute staff, students and others who transact business with the Institute and on behalf of the Institute.

The policy covers:

- Definition of fraud
- General principles
- Procedures for reducing the potential for fraudulent activity
- Responsibilities of Management and Staff Members
- Procedures for reporting and investigating suspected fraud Disciplinary Procedures

1.2. Repeal of all existing policies

This Policy supersedes and repeals all previous policies, procedures and practices in respect of the detection, reporting and management of instances of fraud or suspected fraud.

2. Scope

2.1. Application

This policy applies to any fraud, or suspected fraud, involving institute employees and students as well as consultants, suppliers, contractors, external agencies and any other parties with a business relationship with IADT. The policy relates to fraud, or suspected fraud, involving the Institute's funds, assets and records and is applicable to all IADT and IADT controlled funds and assets including research grants and consultancy projects administered by the Institute. The policy also applies to any subsidiary companies established by IADT¹.

¹ IADT does not currently have any subsidiary Companies, this Policy will apply to any that are established.

2.2. Institute Policies

Staff Members should ensure that they are familiar with other relevant Institute policies, procedures and regulations, including but not limited to:

- IADT Staff Policies
- IADT Staff Code of Conduct
- IADT Financial Policies and Procedures
- IADT Procurement Policy
- IADT Credit Card Policy
- IADT Mutual Respect Policy
- IADT Appropriate and Acceptable Use of ICT Policy
- IADT Protected Disclosures Policy
- IADT Staff Grievance Policy
- IADT Staff Disciplinary Policy
- IADT Complaints Policy

3. Definitions

3.1. Fraud

The term 'fraud' is used to describe acts of dishonesty such as deception, bribery, forgery, extortion, corruption, theft, falsification, embezzlement, misappropriation, false representation, concealment of material facts, false pretence, false accounting and conspiracy and/or collusion in any of the foregoing. For the purposes of this policy, the term 'fraud' also includes attempted fraud.

Legal definitions of fraud tend to identify that the dishonesty must be made knowingly or believing the act or statement not to be true and honest, or being reckless and/or careless as to whether the act or statement is true or false².

3.2. Advantage

For practical purposes fraud may be defined as the use of deception to obtain an advantage or attempt to obtain an advantage, avoid an obligation or cause loss to another party.

3.3. Activities and Behaviours

It is not possible to give an exhaustive listing of the activities and behaviours which constitute fraud. Some of the following are examples of fraudulent behaviour with a more detailed but non-exhaustive list contained in Appendix A:

- Theft, misappropriation or unauthorised use of Institute property;
- Claiming payment for goods not received, services not performed, time not reported.

² Lord Hershall in *Derry v Peake* (1889) 14 App Cas 337

- Submitting false, exaggerated or misleading claims for reimbursement of expenses;
- Purchasing items for personal use with Institute funds;
- Submitting false, exaggerated or misleading documents in respect of absences from work including but not limited to; medical records, social welfare records;
- Submitting false, exaggerated or misleading documents in respect of the IADT Staff Recruitment Process and or Student Registration Process;
- Submitting any document that has been falsified in support of any claim or to obtain any benefit including non-financial benefits;
- Forging or falsifying any documents or altering any documents without proper authority;
- Offering or accepting gifts or hospitality in return for favourable decisions;
- Knowingly creating false or misleading financial reports;
- Knowingly misrepresenting the findings of research and/or research surveys for the purposes of an academic, financial or reputational gain.

In the event of a question arising as to whether an action could constitute a fraud, guidance may be sought from the Secretary/Financial Controller.

4. General Principles

It is IADT's policy to investigate all cases of suspected fraud and, when appropriate, to pursue legal remedies available under the law.

Any act of fraud ascertained upon investigation, pursuant to a criminal conviction, or through written acknowledgment by the employee(s) and/or student(s) concerned, shall result in the appropriate disciplinary and legal actions against the employee(s), student(s) and/or entities, to include the possibility of termination of employment, deregistration from the Institute, cancellation of any contract, restitution to IADT and/or forwarding information to the appropriate authorities for criminal prosecution. The repayment of losses will be sought in all cases and the Institute would normally expect to recover all costs in addition to the recovery of losses.

Any individual who is the subject of any inquiry under this Policy will be afforded all rights of natural justice as provided for within the Institute's Disciplinary Procedures.

5. Reducing the potential for fraudulent activity

IADT recognises that instances where fraudulent activity may be suspected is rare and that staff members of IADT are fully committed to advancing the Institute and to achieving its strategies and objectives. However, there is always a risk that there is potential for fraudulent activity to happen and therefore IADT employs a range of actions to reduce this potential including written policies and procedures, requiring transactions to be properly authorised and providing for sufficient segregation of duties.

Those members of staff with management or supervisory responsibilities should ensure that all members of staff in their department are aware of IADT policies and procedures and that these policies and procedures are adhered to at all times.

6. Responsibilities

Managers and employees at all levels are responsible for exercising due diligence and control to prevent, detect and report acts of fraud or suspected fraud, while recognising that it would be a unusual event.

6.1. Responsibility of Management

Managers are required to be familiar with the types of improprieties that might occur in their area and to be alert for any indication that improper activity, misappropriation or dishonest activity is or was in existence in their area. Managers are also responsible for implementing systems of control to avoid such occurrences.

All managers are required to support and work with those employees, departments and law enforcement agencies involved in the detection, reporting and investigation of dishonest or fraudulent activity including the prosecution of offenders. If a fraud is detected in an area, the manager is responsible for taking appropriate corrective measures to ensure adequate controls exist to prevent reoccurrence of improper actions.

6.2. Responsibility of Employees

All employees are required to conduct their Institute business in such a way as to prevent fraud occurring in the workplace. Employees must also be alert to the possibilities for fraud and be alert for any indications that improper or dishonest activity is taking place.

7. Reporting Procedures

Members of staff should notify their Head of Department / Function or immediate supervisor in writing or by e-mail of any suspected impropriety without delay. The person receiving such a notification should notify the Secretary/Financial Controller and/or President without delay.

On receipt of a notification the Secretary/Financial Controller will bring the matter to the attention of the Head of Internal Audit, and where appropriate, to the Chairperson of the Audit & Risk Committee of the Governing Body³.

In circumstances where members of staff are unable to report the matter to their Head of Department / Function or immediate superior, they should themselves report the matter to the Secretary/Financial Controller or President. Where either the Secretary/Financial Controller and/or President are the subject of the alleged or

³ Details of the Chair of the Audit & Risk Committee are available from the President's Office or on the IADT Website.

suspected fraud, the notification should be made to the Finance Manager, who will notify the Chairperson of the Audit & Risk Committee of the Governing Body.

It is important that delays in notifying the relevant Managers and the Audit & Risk Committee are minimised wherever possible. Unnecessary delays in making notifications and/or in conducting enquiries increases the possibility of additional losses to the Institute and/or impeding the process of enquiries and investigations.

In making a report, members of staff must take care to avoid making incorrect accusations or alerting suspected individuals. The good name and reputation of individuals, the subject of suspicion of fraud, is not undermined where an honest and reasonable report of suspicious circumstances is made.

This Policy encourages an individual to put their name to the concern raised where possible. While, anonymous reporting is discouraged, where such concerns are supported by evidence, they may form the basis of an investigation. In considering anonymous concerns raised, the Institute will take into account factors such as:

- The seriousness of the issues raised;
- The credibility of the concern;
- The likelihood of being able to investigate and confirm the allegation (using alternative sources if possible); and
- The requirements of fairness with reference to any individual named in the disclosure.

The provisions of any IADT Disclosures Policy will apply to reports made under this Policy.

After initial reporting, employees and managers are required to refrain from discussing the incident, facts, suspicions or allegations with anyone inside or outside the Institute unless specifically directed to do so by the Secretary/Financial Controller.

A process checklist notifications and reporting of suspicions is set out in Appendix 2 and operates as a guide for staff, Managers and/or investigators. This is a guide only and the individual circumstances of any case will differ from case to case.

8. Investigations

8.1. Procedure

Investigative activity, where required, will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the Institute.

The Secretary/Financial Controller, working in conjunction with the Head of Internal Audit⁴ and the Chairperson of the Audit & Risk Committee of the Governing Body where appropriate, has primary responsibility for the conduct of investigations of all suspected fraudulent acts as defined in the policy. Where it is inappropriate for the Secretary/Financial Controller to be involved, the President may designate an appropriate member of the Executive, who will be designated the authorities ascribed to the Secretary/Financial Controller within this Policy, to assume primary responsibility for reporting and investigating suspected fraudulent acts.

Normally, an investigation will be conducted by the Institute's Internal Auditors or by an Investigation Team convened by the Secretary/Financial Controller for that purpose. Membership of this Team, which may include external specialists, will be determined by the Secretary/Financial Controller, in conjunction with the President and/or the Chairperson of the Audit & Risk Committee and will be dependent on the nature and context of the investigation being undertaken. Depending on the seriousness of the issue, investigations may be conducted by IADT Managers trained for the purpose or for more serious issues, external authorities such as the Gardai may immediately be notified.

Any person subject to such an investigation will be afforded an opportunity to provide an explanation as part of the investigation process and will be afforded all rights of natural justice as provided for within the Institute's Disciplinary Procedures.

It would normally be expected that an initial investigation should be completed within 10 working days of its commencement. Formal and/or external investigations may take longer to conclude, but provision for interim reports will be included within the Terms of Reference for any investigation.

8.2. Authorisation

In conducting an investigation, the Internal Auditors or the Investigation Team will have a written Terms of Reference, which may include:

- Details of the allegation;
- Timelines for completion;
- Requirements for interim reports;
- Details of the mechanism for issuing the report;
- Details of access to all Institute records and premises, which may be free and unrestricted;
- Details of the investigators authority to examine, copy and/or remove all or any portion of the contents of files, desks, cabinets and other storage facilities on the premises with or without prior knowledge or consent of any individual who may use or have custody of any such items or facilities when it is within the scope of their investigation;

⁴ The Head of Internal Audit may be an appropriate employee of the contracted Internal Audit Professional Service engaged by IADT.

- Details of the investigator's authority to examine, copy and/or remove all or any portion of the contents of any computer, laptop, tablet, mobile phone, electronic storage device, e-mail account, social media account, network drive with or without prior knowledge or consent of any individual who may use or have custody of any such items or facilities when it is within the scope of their investigation.
- Details of the investigator's authority to interview and question all relevant staff members, contractors and their employees and/or other third parties.

The specifics of the Terms of Reference will be detailed and separate for each investigation and the level of authority for the items above will depend on the status of the investigation whether preliminary or full. Where allegations of fraud are notified to external agencies, the powers to conduct investigations will be a function of the powers assigned to that agency and their personnel under law.

8.3. Inquiries

Inquiries from the suspected individual, his/her representatives, or other parties concerning the activity under investigation, should normally be directed to the Secretary/Financial Controller. No information concerning the status of an investigation should be divulged.

Any individual who is the subject of any inquiry under this Policy will be afforded all rights of natural justice as provided for within the Institute's Disciplinary Procedures.

8.4. Investigation Findings

On completion of the preliminary investigation of the facts, the Internal Auditors or Head of the Investigation Team shall present a written report to the Secretary/Financial Controller and to the Chairperson of the Audit Sub-committee.

8.5. Confidentiality

Investigation results cannot be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct and to protect the Institute from potential civil liability.

9. Disciplinary Procedures

Following completion of the investigation and where the facts as established warrant further action, the matter may be referred in accordance with IADT's established disciplinary procedures or to the Gardaí or other appropriate authorities.

Appendix A

Examples of Fraudulent Behaviour

Some of the following are examples of fraudulent behaviour, this list is indicative only and not exhaustive:

Financial Matters

- Theft or misappropriation of the Institute's funds, securities, materials, supplies, assets or other property;
- Procuring or obtaining goods, services or seeking access to finance or credit in the name of the Institute without authority;
- Claiming payment for goods not received or services not performed;
- Claiming payment for time not worked either in cash or time-in-lieu;
- Submitting false, exaggerated or misleading claims for reimbursement of expenses;
- Submitting false, exaggerated or misleading claims for grants or student supports;
- Purchasing items for personal use with Institute funds;
- Impropriety in the handling or reporting of money or financial transactions;

Ethical Matters

- Deriving secret profit from the discharge of one's duty as an employee or contractor of the Institute;
- Accepting or seeking anything of material value from contractors, suppliers or persons providing goods or services to the Institute;
- Offering or accepting gifts or hospitality in return for favourable decisions;
- Accepting bribes or commissions from a third party;
- Payment of excessive prices or fees in return for an opportunity to procure items for personal use at more favourable prices from the supplier;
- Payment of excessive prices or fees where justification thereof is not documented;
- Preferentially procuring materials or supplies from suppliers;

Documentary Matters

- Forgery or alteration of any document or accounting belonging to the Institute;
- Knowingly creating false or misleading financial reports;
- Establishing a trading or business account under the aegis of the Institute using false names;
- Falsification of any marks, scores, exam or assessment results including but not limited to CAO and Portfolio scores;
- Altering any record without appropriate authority;
- Issuing any document or record without appropriate authority;
- Submitting any document that has been falsified;
- Making any claim for support or in support of any application that is false, exaggerated or misleading;
- Concealing any information in the context of any application and/or claim;
- Falsification of the results of any survey or the outcome of any research;
- Unauthorised disclosure of confidential or proprietary information to outside parties;

General Matters

- Any dishonest or fraudulent act;
- Forging, falsification or altering documents;
- Wrongful acts or defaults which confer an unauthorised benefit on the person concerned or on a third party;
- Willful destruction, removal or inappropriate use of records, furniture, fixtures, equipment, and property and/or any similar or related inappropriate conduct;
- Utilising Institute time and resources for personal business or for personal financial gain;
- Removing Institute property from the campus without proper written authorisation;
- Misappropriation of an Institute business opportunity;

HR Matters

- Providing false, exaggerated or misleading information or concealing information in the context of any pre-employment or other medical examination requested by the Institute;
- Providing false certification of academic qualifications;
- Without prior written approval, taking payment or deriving benefit directly or indirectly for services rendered to a third party whilst a full-time employee of the Institute;
- Drawing a salary from the Institute whilst absent without authorisation from work; Submitting false, exaggerated or misleading documents in respect of absences from work including but not limited to; medical records, social welfare records.

Appendix B

Checklist for Notifications, Reporting and Investigations

Initial action checklist upon discovering a potential fraud:

1. You should alert your manager of your suspicions, if your suspicions relate to your manager or other individuals within your line management structure you should alert one of: the Secretary/Financial Controller, the President or the Chairperson of the Audit & Risk Committee of the Governing Body. Any notification made in this regard will be considered as a Protected Disclosure under the Institutes Protected Disclosure Policy.
2. You should document the relevant dates, times and details of your initial suspicions, including the details of any documents or records that alerted you.
3. You should make notes of all observations and actions – if something is worth taking a mental note, it is worth a written note.
4. You should maintain confidentiality (only inform those people who need to know about the suspected act). Unwarranted disclosure can seriously damage the reputation of innocent individuals and or potential successful investigations. You **must not** confront the suspect(s).
5. You should write out in as much detail as possible the suspected act or wrongdoing including:
 - a. What is alleged to have occurred
 - b. Who is alleged to have committed the act
 - c. Is the activity continuing
 - d. Where did it occur
 - e. What is the value of the loss or potential loss if this is known to you.
 - f. Who knows of the activity
6. You **must not** conduct any enquiries or investigations, these will be a matter for the relevant authorities
7. You **must not** remove any documents or files from the Institute other than the notes that you have made yourself.
8. You **must not** interfere with or impede any process or system unless specifically authorised to do so.

Secondary actions on investigating a potential fraud

1. An Investigator or other authorised person should identify and list all documentary and other evidence connected to the activity:
 - g. Invoices
 - h. Contracts
 - i. Purchase orders
 - j. Cheques
 - k. Computers
 - l. Credit card statements
 - m. Other documents and files as appropriate
2. An Investigator or other authorised person should obtain evidence and place in a secure area. (only where it is possible without alerting any suspects)
3. An Investigator or other authorised person should protect evidence from damage or contamination

4. An Investigator or other authorised person should list each item individually taking note of acquisition (incl. time, date and location) and where the item was securely stored
5. An Investigator or other authorised person should identify all potential witnesses
6. Unless electronic evidence is in the process of being destroyed an Investigator or other authorised person **must not** go into the suspect/target computer systems
7. An Investigator or other authorised person should if possible, secure and/or remove suspect's access to relevant computers/systems. Do not allow IT department to examine computer
8. An Investigator or other authorised person should consider other potential suspects and extent of fraud
9. An Investigator or other authorised person should prepare a report and issue same to the relevant Institute and/or investigative authority.