Policy Title:	Data Breach Policy and Procedures
Description:	The purpose of this policy is to provide Marino Institute of Education's intent, objectives and procedures regarding data breaches involving personal information. As we have obligations under the GDPR, we also have a requirement to ensure that adequate procedures, controls and measures are in place and are disseminated to all employees; ensuring that they are aware of the protocols and reporting lines for data breaches. This policy details our processes for reporting, communicating and investigating such breaches and incidents.
Author (Position):	DPO
Version:	1
Approved By:	Governing Body
Policy Approval Date:	January 2021
Date of Next Policy Review:	January 2024 (or as necessary)

Data Breach Policy and Procedures

1. Policy Statement

Marino Institute of Education *(hereinafter referred to as 'MIE')* is committed to our obligations under the regulatory system and in accordance with the GDPR, and maintain a robust and structured programme for compliance and monitoring. We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary. However, we recognise that breaches can occur, hence this policy states our intent and objectives for dealing with such incidents.

Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from any risks associated with processing data. The protection and security of the personal data that we process is of paramount importance to us and we have developed data specific protocols for any breaches relating to the GDPR and the data protection laws.

2. Purpose

The purpose of this policy is to provide MIE's intent, objectives and procedures regarding data breaches involving personal information. As we have obligations under the GDPR, we also have a requirement to ensure that adequate procedures, controls and measures are in place and are disseminated to all employees; ensuring that they are aware of the protocols and reporting lines for data breaches. This policy details our processes for reporting, communicating and investigating such breaches and incidents.

3. Scope

This policy applies to all staff within MIE (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with MIE in Ireland or overseas). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4. Data Security & Breach Requirements

MIE's definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples of data incidents (the "Data Incident") that may be personal data breaches include but are not limited to:

(a) loss, theft or misplacement of IT equipment or devices containing Personal Data e.g. smartphone, laptop or USB key

(b) loss, theft or misplacement of briefcase or folder containing Personal Data in physical hardcopy form

(c) human error resulting in email or post containing Personal Data being sent to an unintended recipient

(d) unauthorised access to automated or manual Personal Data as a result of a break-in to MIE's premises

(e) unauthorised access to Personal Data as a result of a breach of access controls

(f) an attack by a "Hacker", i.e. unauthorised access to MIE's computer network, which may consist of a deliberate interruption to IT network services or penetration of the IT network or system, by an unauthorised party with the intention of obtaining information, destroying data or preventing access to data

(g) unforeseen circumstances such as a flood or fire, in particular where Personal Data is not accessible either temporarily or permanently

(h) unauthorised access to Personal Data where information is obtained by deception

(i) in certain circumstances, where there is a loss of access to or availability of Personal Data (temporarily or permanently), for example where Personal Data has been deleted either accidentally or by an unauthorised person and the data cannot be restored

(j) unauthorised alteration of student's personal data without prior consent.

Whether the Data Incident giving rise to the suspected Data Breach involves Personal Data must be determined on a case-by-case basis. If a Data Incident does not involve Personal Data, it is not a Data Breach. Furthermore, not all Data Incidents involving Personal Data will

be Data Breaches. For example the loss or compromise of Personal Data may not qualify as a Data Breach where:

(a) there is limited risk to the individuals, their rights or freedoms, resulting from the Data Incident;

(b) the Personal Data is securely encrypted or anonymised such to make the Personal Data unintelligible; and/or

(c) there is a full, up-to-date back-up of the Personal Data (in cases of accidental destruction).

Alongside our *'Privacy by Design'* approach to protecting data, we also have a legal, regulatory and business obligation to ensure that personal information is protected whilst being processed by MIE. Our technical and organisational measures are detailed in our Data Protection Policy & Procedures and Information Security policies.

We carry out information audits to ensure that all personal data processed by us is adequately and accurately identified, assessed, classified and recorded, and risk assessments that assess the scope and impact of any potential data breach; both on the processing activity and the data subject. We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risks, including *(but not limited to*):

- pseudonymisation and encryption of personal data
- restricted access and biometric measures
- reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- audit procedures and stress testing on a regularly basis to test, assess, review and evaluate the effectiveness of all measures in compliance with the data protection regulations
- frequent and ongoing data protection training programs for all employees
- staff awareness and training courses, and assessments to ensure a high level of competency, knowledge and understanding of the data protection regulations and the measures we have in place to protect personal information

- reviewing internal processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal; these processes should be checked and authorised by the Data Protection Officer

4.1 Objectives

- to adhere to the GDPR and Irish Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches;
- to develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information;
- to utilise information audits and risk assessments for mapping data and to reduce the risk of breaches;
- to have adequate and effective risk management procedures for assessing any risks presented by processing personal information;
- to ensure that any data breaches are reported to the correct regulatory bodies within the timeframes set out in any regulations, codes of practice or handbooks;
- to use breach investigations and logs to assess the root cause of any breaches, and to implement a full review to prevent further incidents from occurring;
- to use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected;
- to protect consumers, clients and employees, including their information and identity;
- to ensure that where applicable, the Data Protection Officer is involved in and notified about all data breaches and risk issues;
- to ensure that the Supervisory Authority (Data Protection Commission) is notified of any data breach (*where applicable*) with immediate effect, or at the latest within 72 hours of MIE having become aware of the breach.

5. Data Breach Procedures & Guidelines

MIE has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Procedures and guidelines for identifying, investigating and notification of breaches are detailed below. Our documented breach incident policy aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

5.1. Breach Monitoring & Reporting

MIE has appointed a Data Protection Officer (DPO) who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to the DPO with immediate effect, whereby the procedures detailed in this policy are followed.

All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure that gap and pattern analyses are available and used. Where a system or process failure has given rise to a data breach, revision to any such process is recorded in the Change Management and Document Control records.

5.2. Breach Incident Procedures

i. Identification of an Incident

As soon as a data breach has been identified, it is reported to the direct line manager and the reporting officer (the DPO) immediately, so that breach procedures can be initiated and followed without delay.

Reporting incidents in full and with immediate effect is essential to the compliant functioning of MIE and is not about apportioning blame. These procedures are for the protection of the Institute, its staff, students, and third parties. They are of the utmost importance for legal regulatory compliance.

As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document as they are required to be assessed on a case by case basis; however, the aim of any such measures should be to stop any further risk/breach to the organisation, staff, student, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident form in all cases.

ii Breach Recording

MIE is required to maintain a log of all Data Breaches and Data Incidents (including those not requiring notification to the DPC and/or a communication to individuals). The log entry

must specify: (i) the facts relating to the Data Breach or Data Incident; (ii) its effects; and; (iii) the remedial action taken by MIE.

MIE utilises a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder (electronic or hard-copy) and reviewed against existing records to ascertain patterns or reoccurrences.

In cases of data breaches, the DPO is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and documentation purposes.

If applicable, the Supervisory Authority (DPC) and the data subject(s) are notified in accordance with the GDPR requirements (*refer Section 6 of this policy*). The Supervisory Authority protocols are to be followed and their online *Security Breach Notification Form* should be completed and submitted. In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

5.3. Breach Risk Assessment

i. Human Error

Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee(s) held.

A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed in accordance with MIE's Risk Assessment Procedures. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause.

It is recommended that a data breach is reported immediately, at which time the DPO will manage the investigation in consultation with the relevant department.

ii. System Error

Where the data breach is the result of a system error/failure, the IT team are to work in conjunction with the DPO to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system(s) involved, and a full review and report to be added to the Breach Incident Form.

Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident:

- attempting to recover any lost equipment or personal information;
- shutting down an IT system;
- removing an employee from their tasks;
- the use of back-ups to restore lost, damaged or stolen information;
- making the building secure;
- if the incident involves any entry codes or passwords, then these codes must be changed immediately and members of staff informed.

iii. Assessment of Risk and Investigation

The DPO should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches. If it is determined that incident does or may amount to a Data Breach, the next step is to assess the risks to individuals (for example, identity theft, fraud, reputational damage). This assessment should, in particular, consider the likelihood of risks taking place and the severity of such risks is to be categorised as ***no risk / risk / high risk*** in accordance with the detailed criteria below:

The lead investigator should look at: -

- Type of breach: A Data Breach may include any unauthorised or accidental disclosure, loss, destruction, damage or any other form of unauthorised, accidental or unlawful access to, collection, use, recording, storing or distributing of Personal Data. What type of Data Breach has or may have occurred? Does the breach consist of a breach of confidentiality relating to Personal Data? Is there a temporary or permanent lack of availability or access to Personal Data and if temporary, how long will it be before it is restored?
- The type of information involved: Is the relevant Personal Data sensitive in nature? The more sensitive the Personal Data the higher the risk of the Data Breach. The utility of the relevant information may also indicate a higher risk to the affected individuals.
- Scale and volume of Personal Data affected: The higher the volume of the Personal Data records and the number of individuals potentially affected will usually create a higher risk.
- Ease of identification**:** The ease of identifying the relevant individuals based on the Personal Data will likely increase the risk of identity theft, fraud and reputational damage in particular.
- what protections are in place (e*g encryption*)? Are the risks arising from the breach limited as a result of inherent security measures, such as encryption, where the confidentiality of the key is still intact and the data is unintelligible to a third party?
- what happened to the information/where is it now?
- whether there are any wider consequences/implications to the incident
- Containment measures: Have any containment measures been implemented which mean that the Data Breach is unlikely to present a risk to the individuals affected?
- Other factors: Other relevant factors in assessing the risk to individuals is whether those individuals affected by the Data Breach have any special characteristics (for example children or vulnerable adults).
- Severity of risk: Based on the above criteria and any other relevant factors, MIE should assess the severity of the risk in terms of the potential consequences to the individuals affected by the Data Breach.
- Likelihood of the risk(s) materialising: Once the Data Breach has occurred, MIE must objectively assess the likelihood of the potential risks actually materialising and this should form part of the risk assessment.

The appointed lead should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

6. Breach Notifications

MIE recognises our obligation and duty to report data breaches in certain instances. All staff have been made aware of the Institute's responsibilities, and we have developed strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay.

6.1. Supervisory Authority Notification

The Supervisory Authority is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, would lead to significant detrimental effects on the individual.

Where applicable, the Supervisory Authority is notified of the breach no later than 72 hours after MIE becomes aware of it, and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be *unlikely* to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

The notification to the Supervisory Authority will contain: -

- a description of the nature of the personal data breach;
- the categories and approximate number of data subjects affected;
- the categories and approximate number of personal data records concerned;
- the name and contact details of our DPO and/or any other relevant point of contact (*for obtaining further information)*;
- a description of the likely consequences of the personal data breach.

- a description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

Breach incident procedures are always followed and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Supervisory Authority if requested.

Where MIE acts in the capacity of a processor, we will ensure that controller is notified of the breach without undue delay. In instances where we act in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obligated to notify us without delay after becoming aware of a personal data breach.

6.2. Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

The notification to the Data Subject shall include:

- the nature of the personal data breach;
- the name and contact details of our DPO and/or any other relevant point of contact (*for obtaining further information)*;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*.

MIE should determine the most appropriate and effective means of communicating the Data Breach to the affected individuals, if necessary engaging the assistance of communications advisors. The notification to Data Subjects should be made without undue delay (to be determined on a case-by-case basis and after consultation with the DPC if appropriate).

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it (ie encryption, data masking etc), or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

6.3 Other Notification requirements

MIE should consider whether, and seek advice as appropriate, as to whether there are any other relevant notification requirements are required (such as to the Gardaí, Central Bank, etc.). The timing of any such notification will depend on the nature of the Data Breach and the legal advice provided in relation to the Data Breach.

7. Record Keeping

All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the DPO, and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

8. Responsibilities

MIE will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

The DPO is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.

9. Related Documents

9.1 Data Breach Incident Form

9.2 Data Protection Policy and Procedures