SECTION 9. INFORMATION & DATA MANAGEMENT

9.1 Information Management

9.1.1 Purpose

Reliable information and data are available to facilitate informed decision-making at Fusion Training and Development. The organisation's Information Management Policy enables it to securely control and track information and assist the company in ensuring compliance with statutory and legal regulations. Information and any data pertaining to the operation of the company and all academic-related activities are available in hard copy format and digital format. Fusion Training and Development is transitioning all data to the Cloud.

9.1.2 Policy Statement

This policy outlines Fusion Training and Development's internal and public information systems used to securely collect, process, and apply information to support the development of successful academic programmes and all related activities. It refers to both paper-based and digitally-based records.

The Fusion Training and Development Information Management System infrastructure:

- Supports the company's core functions.
- Ensures the company's continued compliance with relevant legal and regulatory obligations.
- Facilitates accurate reporting to enable specific and prompt decision-making across the company's activities and services.
- Indicates commitment to maintaining a robust information security environment.

Fusion Training and Development is fully compliant with organisational obligations under data protection legislation and the General Data Protection Regulation (GDPR). The policy applies to all staff, learners, stakeholders, and all records and information, in both hard and soft copy.

9.1.3 Responsibility

This policy is the responsibility of the Administrator under the guidance of the Managing Director.

9.1.4 Processes & Procedures

Learner Management System

Fusion Training and Development maintains learner information using a secure, customised learner management system. Information retained includes the learner's:

- Personal details.
- Contact information.
- Assessment results.
- Stages completed.
- Awards conferred.
- Classification of awards.
- Certification results.
- Personal mitigating circumstances detail.
- Communications received from learners.

The Fusion Training and Development Learning Information System has been customised and configured to meet organisation requirements. This secure and comprehensive database system provides Fusion Training and Development with capabilities to:

- Maintain secure and accurate learner records (for current/historical use).
- Produce reports that contribute to internal quality assurance management and improvement procedures.
- Generate data compliance with external regulatory and national systems.
- Generate statistical and other reports to meet internal and external information requirements.

Fusion Training and Development has arrangements and technical expertise in place to facilitate robust server security systems and the automatic backup of data in case of technical failure. Digital information is being stored on a cloud-based system as well as a paper-based one. The company will increasingly work towards digitising all records and cloud storage with appropriate security protocols in place.

Information is maintained securely through protocols of limited access and differing levels of access. Technical support staff, security administrators, system administrators, and others may need special account access privileges compared to typical or everyday users. The provision of administrative and special access accounts with a higher level of access means that granting, controlling, managing, and monitoring these accounts is extremely important to Fusion Training and Development's information security programme.

Management Information Systems

The company's management information system facilitates the storage and retrieval of information as required. The management system enables prompt analysis of key performance indicators and objectives and enables the ongoing monitoring of programs and all associated services (for more information, see Internal Review, Monitoring, and Self-Evaluation Policy).

Information Management for Decision-making

Fusion Training and Development generates reports on learner retention, progression, and completion rates which are used to inform the ongoing monitoring of programmes and all associated services. The Managing Director is responsible for learner feedback surveys and the generation of associated reports. These reports feed into the annual monitoring reports for individual programmes. Reports enable the company to identify influencing factors, determine patterns that assist in benchmarking and inform decision-making, and identify opportunities for additional data analysis that may be of benefit.

Learner achievement reports are generated by the Managing Director for consideration by the Results' Approval Board (RAP). This information details the breakdown of learner performance across individual modules, and final award classification recommendation data will facilitate cross-programme analysis and comparative data. An analysis report is incorporated into monitoring reports, notified to the External Authenticator, and used to inform programme changes, teaching, learning, and assessment strategies, or learner support services.

Records' Maintenance & Retention

Records' retention and management is an important component of the Fusion Training and Development process. The company needs to store and manage information on general operations, student records, and finance as part of day-to-day activities. As part of a retention scheme, classes of documents are retained on different schedules based on various criteria. Fusion Training and Development specific record retention schedules provide a consistent policy regarding the retention and disposal of educational and operational records. Fusion Training and Development sets records' retention schedules to address legal, statutory, and compliance requirements as well as litigation needs, business processes, and data privacy concerns. Storage requirements are coordinated to comply with requirements for record storage.

Fusion Training and Development retention periods are generally determined by:

- Evaluating applicable regulatory, statutory, legal, or general state and federal compliance requirements.
- Determining electronic data components collected, their purpose, and applying the appropriate retention procedure to each class of data asset.
- Identifying other internal or external entities that collect, store, archive, or use Fusion Training and Development information and records.

Fusion Training and Development is committed to developing and enhancing procedures and documentation that implement and maintain the retention requirements as outlined in this policy. Specific procedures do and shall specify the retention time, archival rules, data formats, and the permissible means of storage, access, and encryption (if any).

All staff who create and maintain records as part of their duties are responsible for these records. Fusion Training and Development has arrangements with an external provider (IT specialist) to support and maintain backups of all records held in the learner management system.

The Managing Director is responsible for the secure storage and maintenance of all

assessment documentation and all transfer of third-party information to other accrediting bodies. **Appendix 5** is Fusion Training and Development's current Records' Retention Schedule and is subject to revision as and when legislation and regulations change at national level.

9.2 Privacy Policy

9.2.1 Purpose

This policy explains how and why Fusion Training and Development collects information, what we do with that data, why we use it, and whether or not it is shared with others and for what purpose. It is prepared in the context of current Data Protection legislation.

9.2.2 Consent

By providing us with your information you are indicating your consent for Fusion Training and Development to collect and process your details in the following manner:

The information we collect & how we use it

We process data to perform our business services, to take steps at the individual's request before providing a service, and to comply with our legal and regulatory obligations and for our legitimate interests. Types of people whose data we process:

- Staff including tutors.
- Learners.
- Suppliers.
- Other people whose data is provided to us by one of the other categories e.g. Referees and Emergency Contacts.

Staff including tutors

During the hiring process, the recruitment section outlines the data processes. During a person's employment, we continue to keep the information previously provided and update it as they work with us. We also require employees to provide more personal details as required in their respective position. We will also keep information on employees' attendance and performance.

Learners' Data

Learners are requested to provide information to allow us to take steps before we provide a training service and associated activities e.g. examination and certification.

This information includes the learner's name, address, telephone number, date of birth, email address and training and education details. It also includes one's PPS Number, Course/Programme, Attendance Record, Certification Results, Training Registration Identifier, Training Location, Mode of Delivery, and Financial details relating to Allowances or Benefits, as identified by the appropriate Funding, Certification, or Awarding organisation or employer. We also keep financial details related to one's payment history.

Suppliers

We use and store the personal data of individuals within different organisations (or as an individual) to facilitate the receipt of services and goods from them as one of our suppliers. This includes financial information so that we can pay them and keep the necessary financial records.

Other People whose data is provided to us by one of the other categories e.g. Referees and Emergency Contacts

- If one's information has been provided as a Referee by a prospective or actual Learner/ member of Staff, we use this personal data to contact the person and obtain a reference. This is part of our quality system and so we deem it to be necessary for our legitimate interests.
- If one's information has been provided as an Emergency Contact by a prospective or actual Learner/Student/Trainee, or member of Staff, we use this personal data to contact the person in the case of an accident or emergency. This is part of our quality system and so we deem it to be necessary for our legitimate interests.

Clients

To ensure we meet clients' expectations of our quality service delivery we store personal data and/or the personal data of individual contacts at different organisations as well as keeping records of our conversations, meetings, communications, transactions, and agreements. From time to time, we may also ask people to participate in other activities, which we believe will benefit the organisation or its people. We deem these uses of data to be necessary for our legitimate interests as a company providing training services.

9.2.3 Sharing your information

We will only share information as appropriate with:

- Our clients, where it is an agreed part of our service.
- Prospective employers – to assist them in their hiring processes.
- Individuals and organisations who hold information related to one's reference or application to work with us, this includes past employers, educational establishments and examining/awarding bodies, employment agencies.
- Tax, audit, or other regulatory authorities with whom we have a legal obligation to share information.
- The third-party outsourced IT and data management providers where we have appropriate processing agreements or protections in place.
- Outsourced service providers, where they are contracted to provide services to us and have agreed to meet our stringent data protection contractual requirements.
- Clients overseas [outside the EU] only where one specifically has expressed an interest in working in another country.
- If we merge with or are acquired by another business, we may share personal information with the new owners of the business and their advisers. Individuals will be sent notice of such an event should it occur.

We may disclose or share data to comply with any legal obligation or to enforce or apply our Terms of Business.

9.3 Subject Data Access Request

We must have up-to-date information about a person, their career, and educational accomplishments. Individuals have the right to:

- Confirm the information we hold.
- Modify the information.
- Update it or
- Delete it (to request deletion one must email Fusion Training and Development).

To comply, we ask a person to verify their identity or ask for more information about their request. In some circumstances where we are legally permitted to do so, we may decline the request and we will explain why.

Note: We do not provide the following types of information in response to a data access request: Information about other people; Opinions given in confidence; Repeat requests or privileged information. Other types of information may also be exempt under data protection laws (e.g. data relating to the commission of offences or estimates of damages).

9.4 Opt-Out

If a person no longer wishes to be registered with us, they can let us know at any time.

The person is asked to send an email to Fusion Training and Development and we will remove their details.

9.5 Data Subject Erasure Request Policy

9.5.1 Purpose & Scope

The General Data Protection Regulation provides individuals with rights in connection with personal data held about them. It provides those individuals with a right of access to that data subject to the rights of third parties and the satisfaction of several criteria. This procedure defines the process to follow when a request for access to personal data is received. We understand that failure to comply with the provisions of the Data Protection legislation in responding to requests may render Fusion Training and Development, or in certain circumstances the individuals involved, liable to prosecution as well as giving rise to civil liabilities.

9.5.2 Responsibilities & Definitions

A **Data Protection Officer** is responsible for ensuring that statutory and regulatory obligations concerning the GDPR are adhered to. (Fusion Training and Development has delegated this responsibility to the Administrator).

Data Protection Commissioner is Ireland’s independent authority set up to promote access to official information and protect personal information.

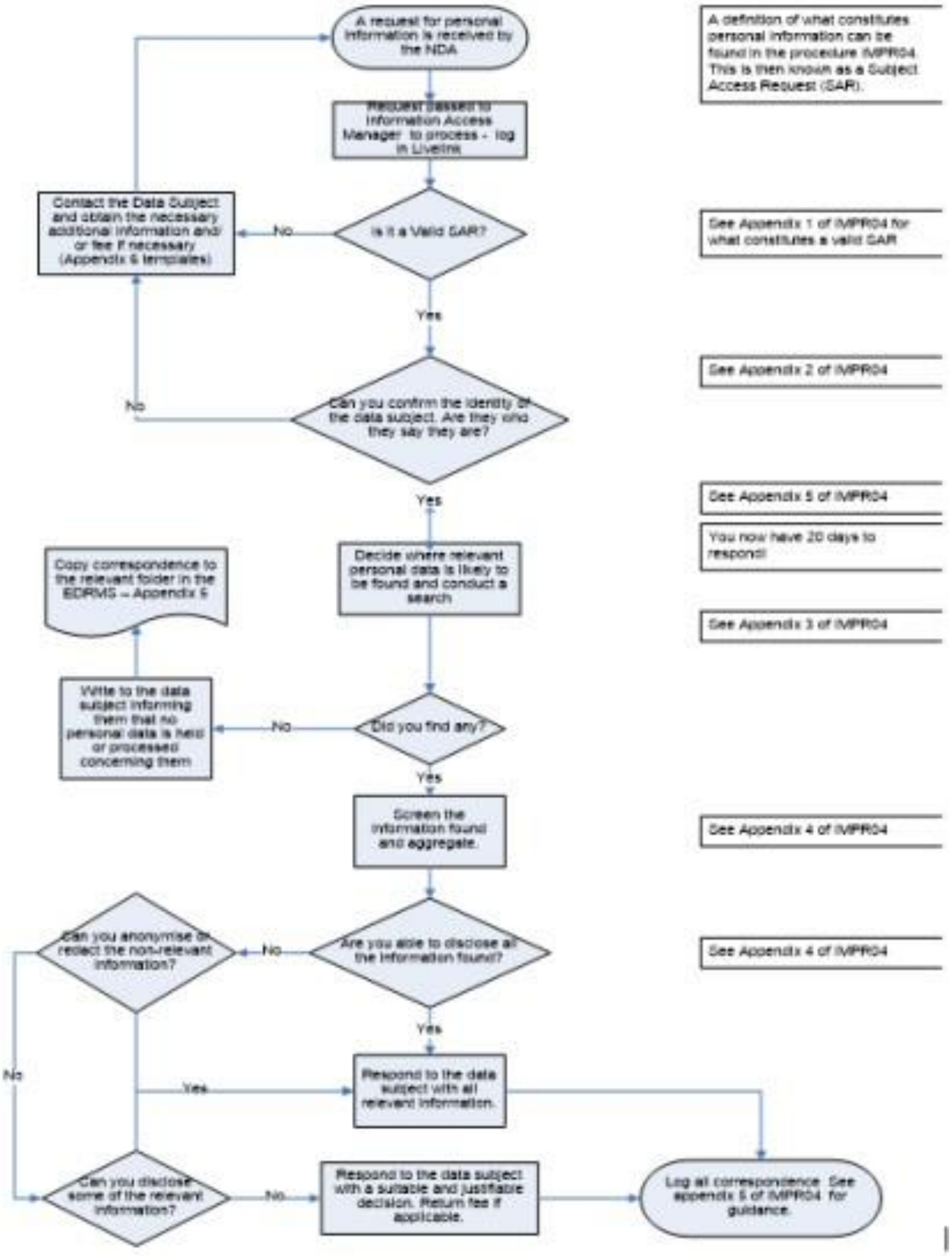
Data Controller is the person or organisation that determines the purposes for which and how any personal data are or are to be, processed. In our case, Fusion Training and Development is the registered Data Controller.

Data Processors are any individual or company who records and/or processes personal data in any form on behalf of Fusion Training and Development and therefore subject to the requirements of this policy. Compliance with this policy is normally managed by contract.

Fusion Training and Development permanent and temporary employees, contractors, and consultants are responsible for incorporating this procedure and its associated policy into their working practices.

The definitions of the terms used in this procedure are as defined in the Data Protection Policy which should be read in conjunction with this procedure.

9.5.3 Procedure


A request for personal information is received by the NDA
Request passed to Information Access Manager to process - log in Livelink
Is it a Valid SAR?
No
Contact the Data Subject and obtain the necessary additional information and/ or fee if necessary (Appendix 6 templates)
Yes
Can you confirm the identity of the data subject. Are they who they say they are?
No
Yes
Decide where relevant personal data is likely to be found and conduct a search
Copy correspondence to the relevant folder in the EDRMS – Appendix 6
Did you find any?
No
Write to the data subject informing them that no personal data is held or processed concerning them
Yes
Screen the information found and aggregate.
Are you able to disclose all the information found?
No
Can you anonymise or redact the non-relevant information?
Yes
Respond to the data subject with all relevant information.
No
Can you disclose some of the relevant information?
No
Respond to the data subject with a suitable and justifiable decision. Return fee if applicable.
Log all correspondence. See appendix 5 of IMPR04 for guidance.
A definition of what constitutes personal information can be found in the procedure IMPR04. This is then known as a Subject Access Request (SAR).
See Appendix 1 of IMPR04 for what constitutes a valid SAR
See Appendix 2 of IMPR04
See Appendix 5 of IMPR04
You now have 20 days to respond!
See Appendix 3 of IMPR04
See Appendix 4 of IMPR04
See Appendix 4 of IMPR04

9.5.4 Documentation

- Records of communications relating to a subject access request (retained for 5 years).
- Records of communications resulting in an action to cease processing personal data (retained for 5 years).

9.6 Additional Considerations

These will be detailed as and when they arise and will be communicated as appropriate to relevant stakeholders interacting with Fusion Training and Development.

9.7 Policy Compliance

Compliance Measurement

Management verifies compliance with this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Managing Director in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9.8 Data Breach Policy

9.8.1 Purpose

Fusion Training and Development has a robust and systematic process for responding to reported data security incidents and breaches. This policy is designed to standardise the business's response to any reported Breach or Incident and ensure that they are appropriately logged and managed by best practice guidelines. Standardised processes and procedures help to ensure that Fusion Training and Development can act responsibly, respond effectively, and protect its information assets to the best possible extent.

9.8.2 Overview

Data breaches are increasingly common occurrences whether caused by human error or malicious intent. Fusion Training and Development operations rely on the proper use of confidential information daily. Managing risk and responding in an organised way to Incidents and Breaches is key to operations and required by law.

9.8.3 Scope

This policy applies to all Fusion Training and Development personnel.

9.8.4 General Information

A 'Data Security Incident' or 'Incident' means an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorised access, loss, disclosure, modification, disruption, or destruction of communication or information resources of the company.

Common examples of Data Security Incidents include, but are not limited to, any of the following:

- Successful attempts to gain unauthorised access to the company's system, employees, contractors, or learner's personal information regardless of where such information is located.
- Unwanted disruption or denial of service.
- The unauthorised use of a company system for the processing or storage of confidential information.
- Changes to Fusion Training and Development's system hardware, firmware, or software characteristics without the company's knowledge, instruction, or consente.
- Loss or theft of equipment where confidential information is stored.
- Unforeseen circumstances such as a fire or flood that could lead to the loss or misuse of confidential information.
- Human error involving the loss or mistaken transmission of confidential information.
- Hacking, social engineering, phishing, or other subversive attacks where information is obtained by the deceitful practice.

A "Data Security Breach" or "Breach" is any Incident where Fusion Training and Development cannot put in place controls or take action to reasonably prevent the misuse of confidential information. A breach is also an incident where data has been misused.

Adopting a standardised and consistent approach to incident management shall ensure that:

- Incidents are reported promptly and can be properly investigated.
- Incidents are handled by appropriately authorised personnel.
- Appropriate levels of management are involved in response management.
- Incidents are recorded and documented.
- Organisational impacts are understood, and action is taken to prevent further damage.

- Evidence is gathered, recorded, and maintained in a form that will withstand internal and external scrutiny.
- External agencies, customers, and data users are informed as required.
- Incidents are dealt with promptly and normal operations are restored.
- Incidents are reviewed to identify improvements in policies and procedures.

Incidents can occur locally, in the cloud, or through third-party service providers. Reporting and management of incidents can similarly occur. Third-party providers are also governed by contract terms and liability as defined in their operational agreements.

Any contract breach that results in the misuse or unauthorised access to confidential information by a Service Contract Provider must be handled according to the General Data Protection Regulations.

9.8.5 Data Classifications

Incidents vary in impact and risk depending on several mitigating factors including the content and quantity of the data involved. It is critically important that Fusion Training and Development management respond quickly and identify the data classification of the incident. This allows staff to respond accordingly in a timely and thorough manner.

All reported Incidents are classified below to assess risk and approaches to mitigate the situation. Data classification refers to the following Fusion Training and Development data categories:

Public Data - Information intended for public and community use or information that can be made public without any negative impact on Fusion Training and Development or its customers. Participants' information shall never be considered public data unless the data is Directory Information as defined by Fusion Training and Development Policy.

Confidential/Internal Data - Information of a more sensitive nature to the business and educational operations of Fusion Training and Development. This data represents basic intellectual capital, applications, and general knowledge. Access is limited to only those people that need to know as part of their role within the company. Employees and participants (except PPSNs, financial information, or other critical information) fall within this classification.

Restricted/Highly Confidential Data- Information that, if breached, causes significant damage to Fusion Training and Development's operations, reputation, and/or business continuity. Access to this information is highly restricted. Participants fall into this category of data. Employee or Educator

Financial Information, Social Security Numbers, and other critical information also fall into this classification.

9.8.6 Incident Reporting (incl. GDPR Report)

The following process shall be followed when responding to a suspected incident:

- Reporting and the ensuing investigation must be prioritised.
- Confirmed or suspected incidents shall be reported promptly to the Management. A formal report shall be filed that includes full and accurate details of the incident including who is reporting the incident and what classification of data is involved.
- Once an incident is reported, Management shall conduct an assessment to establish the severity of the incident, the next steps in response, and potential remedies and solutions. Based on this assessment, Management shall determine if this incident remains an incident or if it needs to be categorised as a breach.
- All incidents and breaches are centrally logged and documented to ensure appropriate documentation, oversight, and consistency in response, management, and reporting.
- All Data Breaches relating to participants must be reported to the Data Protection Commission within 72 hours of the breach being discovered. When reporting a Breach, GDPR states you must provide:
    - a description of the nature of the personal data breach including, where possible:
        - the categories and approximate number of individuals concerned; and
        - the categories and approximate number of personal data records concerned.
        - the name and contact details of the data protection officer (if your organisation has one) or another contact point where more information can be obtained.
    - a description of the likely consequences of the personal data breach; and a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.
    - If a breach is likely to result in a high risk to the rights and freedoms of individuals, those concerned must be informed without undue delay. They must:
        i. Describe the nature of the personal data breach and, at least.
        ii. the name and contact details for a point of contact where more information can be obtained.
        iii. description of the likely consequences of the personal data breach.
        iv. and a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, the measures taken to mitigate any possible adverse effects.

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Article 33(4) allows you to provide the required information in phases, as long as this is done without undue further delay. If Fusion Training and Development is acting as a data processor, the requirements on breach reporting should be detailed in the contract between Fusion Training and Development and the Data Controller, and vice-versa (required under Article 28).

9.8.7 Classification

Data Breaches or Incidents shall be classified as follows:

Critical/Major Breach or Incident – Incidents or Breaches in this category deal with Confidential Information or PII and are on a large scale (company-wide). All Incidents or Breaches involving learners' confidential information will be classified as Critical or Major. They typically have the following attributes:

- Any incident that has been has determined to be a breach.
- Significant Confidential Information or personal information loss, potential for lack of business continuity, Fusion Training and Development exposure, or irreversible consequences are iminente.
- Negative media coverage is likely, and exposure is high.
- Legal or contractual remedies may be required.
- Requires significant reporting beyond normal operating procedures.
- Any breach of contract that involves the misuse or unauthorized access to personal information by a Service Contract Provider.

Moderately Critical/Serious Incident – Breaches or Incidents in this category typically deal with Confidential Information and are on a medium scale (e.g. <10 users on the internal network, application or database related, limited exposure). Incidents in this category typically have the following attributes:

- Risk to the company is moderate.
- Third-party service providers and subcontractors may be involved.
- Data loss is possible but localised/compartmentalised, with the potential for limited business continuity losses, and minimised company exposure.
- Significant user inconvenience is likely.
- Service outages are likely while the breach is addressed.
- Negative media coverage is possible but exposure is limited.
- Disclosure of Educator or Employee PII is contained and manageable.

Low Criticality/Minor Incident – Incidents in this category typically deal with personal or internal data and are on a small or individualised scale (e.g. <5 users on the internal network, personal or mobile device related). Incidents in this category typically have the following attributes:

- Risk to the company is low.
- User inconvenience is likely but not damaging to Fusion Training and Development.
- Internal data released but data is not student, employee, or confidential in nature.

- Loss of data is contained on encrypted hardware.
- Incident can be addressed through normal support channels.

9.8.8 Incident Response

Management response to any reported Incident shall involve the following activities:

Assess, Contain & Recover Data

All security incidents have an immediate analysis of the incident and an incident report completed by management or their designee. This analysis includes a determination of whether this incident should be characterised as a breach. This analysis is documented and shared with the Managing Director, the affected parties, and any other relevant stakeholders. At a minimum, the delegated personnel:

Step	Action	Notes
A	***Containment and Recovery:***	***Contain the breach, limit further organisational damage, and seek to recover/restore data.***
1	Breach Determination	Determine if the incident needs to be classified as a Breach.
2	Ascertain the severity of the Incident or breach and determine the level of data involved.	See Incident Classification
3	Investigate the Breach or Incident and forward a copy of the Incident report to the Information Security Team	Ensure investigator has appropriate resources including sufficient time and authority. If PII or confidential data has been breached, also contact the Management. If the Incident or breach is severe, the Managing Director shall be contacted.
4	Identify the cause of the Incident or breach and whether the situation has been contained. Ensure that any possibility of further data loss is removed or mitigated as far as possible. If this loss cannot be mitigated, any Incident will be characterised as a Breach.	Compartmentalise and eliminate exposure. Establish what steps can or need to be taken to contain the threat of further data loss. Contact all relevant departments who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the Incident.
5	Determine depth and breadth of losses and limit exposure/damages	Can data be physically recovered if damaged through the use of backups, restoration, or other means?
6	Notify authorities as appropriate	For criminal activities where the property was stolen or fraudulent activity occurred, contact the appropriate authorities and general counsel. Should the Breach involve participant details that involve a Service Contract Provider, notify Management
7	Ensure all actions and decisions are logged and recorded as part of incident documentation and reporting	Complete the Incident Report and file it with the Management

Assess Risk & Incident Scope

All incidents or breaches have a risk and scope analysis completed by management (delegated as appropriate). This analysis is documented and shared with the IT specialist, the affected parties, and any other relevant stakeholders. At a minimum, the management:

B	***Risk Assessment***	***Identify and assess ongoing risks that may be associated with the Incident or breach***
1	Determine the type and breadth of the Incident or breach	Classify Incident or breach type, data compromised, and extent of the breach
2	Review data sensitivity	Determine the confidentiality, scope, and extent of the Incident or breach.
3	Understand the current status of the compromised data	If data has been stolen, could it be used for purposes that harm the individuals whose identity has been compromised; If identity theft is involved, this poses a different type and level of risk.
4	Document risk-limiting processes or technology components that contain and manage the Incident	Does encryption of data/devices help to limit the risk of exposure?
5	Determine what technologies or processes will mitigate the loss and restore service	Are there backups of the compromised data? Can they be restored to a ready state?
6	Identify and document the scope, number of users affected, and depth of the Incident or breach	How was many individuals' personally identifiable information affected?
7	Define individuals and roles whose data was compromised	Identify all students, staff, districts, customers, or vendors involved in the Incident or breach
8	If exploited, what will the compromised data tell a third party about the individual? Could it be misused?	Confidential Information could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a criminal build up a detailed picture associated with identity theft or fraud.
9	Determine actual or potential harm that could come to any individuals	Identify risks to individuals: Physical Safety Emotional Wellbeing Personal or Business Reputation Financial Implications Identity Concerns A combination of these and other private aspects of their life?
10	Are there wider consequences to consider?	Is there a risk to another business, the state, or loss of public confidence?
11	Are there others who might provide support or advice on risks/courses of action?	Contact all local education providers, agencies, or companies impacted by the breached data, notify them about the Incident and ask for assistance in limiting the scope of the Incident.

Notification & Incident Communications

Each security incident or breach determined to be 'moderately critical' or 'critical' has communication plans documented by management, and their designees to appropriately manage the Incident and communicate progress on its resolution to all affected stakeholders. At a minimum, management:

C	Notification and Communications	Notification enables affected stakeholders to take precautionary steps and allows regulatory bodies to act on the Incident or breach.
1	Are there legal, contractual or regulatory notification requirements associated with the Incident or breach?	Review vendor contracts and compliance terms assure state and federal reporting and notifications are understood. Contact Management.
2	Notify impacted individuals of Incident or breach remedies.	Provide individuals involved in the Incident or breach with mitigation strategies to re-secure data (e.g. change the user ID and/or passwords etc.)
3	Determine Internal Communication Plans	Work with management and provide regular internal updates on the status of Incidents or breaches, remedies underway, and current exposure and containment strategies. This messaging should be provided to all internal state stakeholders and management. Messaging shall be coordinated through management.
4	Determine Public Messaging	Prepare and execute a communication and follow-up plan with management. Communication strategies need to define audience(s), frequency, messaging, and content.
5	Execute Messaging Plan	Working through management, executing the public and internal communication plans. Depending on the nature and scope of the Incident or breach, multiple messages may need to be delivered as well as press and public communique. Minimally notifications should include: ○ A description of the incident or breach (how and when it occurred) ○ What data was involved and whose data was compromised ○ Details of what has been done to respond to the Incident or breach and any associated risks posed ○ Next-steps for stakeholders Fusion Training and Development contacts for the Incident or breach, and follow, and other pertinent information. When notifying individuals, provide specific and clear advice on the steps they can take to protect themselves and what Fusion Training and Development and/or third-party vendor will do to help minimise their exposure. Provide a way in which they can contact Fusion Training and Development for further information or to ask questions about what has occurred (e.g. a contact name, helpline number, or a web page).

Post-mortem Evaluation & Response

Each incident or breach determined to be "moderately critical" or "critical" shall have a post-mortem analysis completed by management and their designees to appropriately document, analyse, and make recommendations on ways to limit risk and exposure in the future. At a minimum, management shall:

D	Evaluation and Response	To evaluate the effectiveness of the business's response to the incident or breach.
1	Establish where any present or future risks lie	Assess and evaluate the root causes of the Incident or breach and any ways to mitigate and/or prevent a similar occurrence.
2	Consider the data and security measures employed	Evaluate, analyse, and document the use cases and technical components of the Incident or breach. Document areas for improvement in environment, technology, or approach that limit future security exposures. Make recommendations as appropriate.
3	Evaluate and identify areas of weakness in existing security measures and procedures	Document lapses in process, procedure, or policy that may have caused the Incident or breach. Analyse and document solutions and remedies to reduce future risks.
4	Evaluate and identify areas of weakness related to employee skills	Assess employee readiness, education, and training. Document and plan for updates in education or procedural changes to eliminate the potential for future Incidents.
5	Report on findings and implement recommendations	Prepare reports and presentations to Finance Council for major incidents or breaches.

.

Incidents or Breaches. An activity log recording the timeline of Incident management is also completed. Reporting and documentation shall be filed and managed through the company's office. Each of these four elements shall be conducted as appropriate for all qualifying.

9.8.9 Audit Controls & Management

On-demand documented procedures and evidence of practice are in place for this operational policy. These include: archived completed incident reports showing compliance with reporting, communication, and follow-through and executed plans for incident management.