Data Security Breach and Reporting Procedure

1. Purpose

This procedure outlines how the College handles data breaches as classified under GDPR. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data. The term 'personal data' means any information concerning or relating to an identified or identifiable individual. Personal data breaches include incidents that are the result of both accidents (such as sending an email to the wrong recipient) and deliberate acts (such as phishing attacks to gain access to customer data). See UPOL020 UniHaven Data Protection Policy Rev 1 and UPOL025 UniHaven Learning Analytics Policy Rev 1 for more information on the type of data that the College collects, why it collects it, whose personal data it is and how it is stored.

The Data Protection Commissioner (DPC) guides data protection breaches on its website, under the section "Personal Data Security Breach Code of Practice". Reference can be found under Article 33 and Article 34. A breach (or potential breach – i.e., when the personal data is "at-risk" of unauthorised disclosure) of personal data should be reported to the DPC as soon as the College becomes aware of the incident and within 72 hours. This timeframe includes weekends and bank holidays. The College must inform affected individuals without undue delay if the data breach is likely to result in a high risk to their privacy. As such, any data breach must be dealt with immediately and appropriately.

A personal data breach occurs in incidents where personal data is lost, destroyed, corrupted, or illegitimately disclosed. This includes, for example, situations where someone accesses personal data or passes them on without proper authorisation, or where personal data are rendered unavailable through encryption by ransomware, or accidental loss or destruction. In short, a personal data breach is a security incident that negatively impacts the confidentiality,

integrity, or availability of personal data, with the consequence that the College is unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 GDPR. It is important to note that whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

2. Target Audience and Staff Involved in Implementation

The Data Protection Officer (DPO) has responsibility for implementing this procedure in conjunction with the CEO and Academic Director for the benefit of those from whom personal data has been collected including students, staff, and stakeholders. The Data Protection Officer (DPO) must be made aware of breaches or potential breaches and will communicate with the DPC as necessary. The DPO is contactable at dpo@unihaven.ie.

3. Documentation

The following guidelines and policies are relevant to the implementation of this policy:

- UPOL020 UniHaven Data Protection Policy Rev 1
- UPOL023 UniHaven Data Retention Policy Rev 1
- UPOL024 UniHaven Data Security Policy Rev 1
- UPOL025 UniHaven Learning Analytics Policy Rev 1
- https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf

UFORM022 UniHaven Personal Data Breach Report Form Rev 1 is used in conjunction with this procedure.

4. Procedure

When reporting to the DPC, the following elements should be taken into consideration:

- The amount and nature of the personal data that has been compromised.

- The action being taken to secure and/or recover the personal data that has been compromised.
- The action being taken to inform those affected by the incident, or the reasons for the decision not to do so.
- The action being taken to limit damage or distress to those affected by the incident.
- A chronology of the events leading up to the loss of control of the personal data.
- The measures being taken to prevent a repetition of the incident.

An incident gives rise to a risk of unauthorised disclosure, loss, destruction, or personal data alteration. In manual or electronic form, the data controller must consider informing those affected. Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. Inappropriate cases, data controllers should also notify organisations that may be in a position to assist in protecting data subjects, including, where relevant, An Garda Síochána, financial institutions etc. It is imperative that all College staff and students immediately report any potential or suspected data breach to dpo@unihaven.ie . If unsure whether an incident is a data breach or not please refer to the guidance set out within this document and consult with the DPO.

This procedure applies to all processors of College-controlled personal data, including:

- Any individual who is employed by the College or is engaged by the College or who has access to college-controlled or processed personal data in the course of their employment.
- Any student who has access to College-controlled or processed personal data during their studies for administrative, research and/or any other purpose.
- Individuals who are not directly employed by the College, but who are employed by contractors (or subcontractors) and who have access to college-controlled or processed personal data in the course of their duties for the college.

This procedure applies to:

- All personal data processed by the College in any format (including electronic and paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically, or accessed remotely.
- Personal data held on all College IT Systems/Servers is managed centrally by our IT provider, and locally by staff.
- Any other IT systems, including email and cloud-based platforms on which College-controlled or processed personal data is processed.

Whether an incident giving rise to the suspected data breach involves personal data must be determined on a case-by-case basis. If an incident does not involve personal data, it is not a data breach per the GDPR definition. Furthermore, not all data incidents involving personal data will be data breaches. For example:

- The personal data is securely encrypted or anonymised to make the personal data unintelligible.
- There is a full, up-to-date backup of the personal data (in cases of accidental destruction).

If there is any doubt as to whether a data breach has occurred, the DPO should be consulted immediately.

Reporting Procedure

If a staff member becomes aware of an actual, potential, or suspected data breach, they must report the incident to their Line Manager immediately. The line manager must then immediately report the incident to the DPO. After reporting the incident, the relevant Line Manager must complete UFORM022 UniHaven Personal Data Breach Report Form Rev 1 (see Appendix) and forward it to the DPO as soon as possible.

The DPO is responsible for keeping a written record of all potential or suspected data breaches that are notified to him/her (including those that are not notified to the Data Protection Commission or the affected individuals). For this purpose, the Personal Data Breach Report Form must be completed satisfactorily. This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to the relevant staff so that prompt and appropriate action can be taken to resolve the incident.

Upon receiving notification of a data breach, the DPO shall, in conjunction with appropriate members of staff, take the following steps when responding to the incident:

Step 1: Identification and initial assessment of the incident

Step 2: Containment & recovery

Step 3: Risk assessment

Step 4: Notification

Step 5: Evaluation & response

Step 1: Identification & initial assessment of the incident

If any staff member considers that a data breach has, or might have, occurred, they must report the incident immediately to their Line Manager who in turn will complete the UFORM022 UniHaven Personal Data Breach Report Form Rev 1. The Personal Data Breach Report Form will assist the DPO in conducting an initial assessment of the incident.

This assessment will consider:

- Whether a data breach has taken place.
- The nature of the personal data involved in the breach (i.e., whether sensitive or confidential personal data is involved).
- The cause of the breach.

- The extent of the breach (i.e., the number of individuals affected).
- The potential harms to which affected individuals may be exposed.
- Any steps that may be taken to contain the breach.

Following this initial assessment of the incident, the DPO may, according to the severity of the incident, consult with the CEO and decide if it is necessary to appoint a group of relevant managers/officers to assist with the investigation and containment process.

Step 2: Containment & recovery

In the event of a data breach, immediate and appropriate steps must be taken to limit the extent of the breach. The data breach owner, with support from the DPO, must quickly take appropriate steps to ascertain full details of the breach, determine whether the breach is still occurring, recover any losses and limit the damage. Steps might include:

- Establish who within the College needs to be made aware of the breach (e.g., IT supplier, particular units) and inform them of their expected role in containing the breach (e.g., isolating a compromised section of the network).
- Establish whether there is anything that can be done to recover any losses and limit the damage caused by the breach.
- Where appropriate, inform the Gardaí (e.g., in cases involving criminal activity).
- If an inappropriate enquiry is received staff should attempt to obtain the enquirer's name/contact details and confirm that they will ring the enquirer back. The CEO should be informed to deal with any media enquiries that may result.
- The use of backups to restore lost, damaged, or stolen information.
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or passwords then these codes must be changed immediately, and the relevant organisations and members of staff informed.

Step 3: Risk assessment

The DPO, in conjunction with relevant staff, will use the information provided in the Personal Data Breach Report Form to fulfil the requirement to assess the potential adverse consequences for individuals, including how likely such adverse consequences are to materialise and how serious or substantial they are likely to be. This assessment should consider the likelihood of risks taking place and the severity of such risks is to be categorised as no risk/risk / high risk under the detailed criteria below:

- 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 distribution 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?
- Nature of personal data: Is the relevant personal data sensitive in nature? The more sensitive the personal data the higher the risk of a 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.
- Security measures: Are the risks arising from the breach limited because 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?
- 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).
- The severity of risk: Based on the above criteria and any other relevant factors, the DPO 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, the DPO must objectively assess the likelihood of the potential risks materialising and this should form part of the risk assessment. An assessment of the risks for the college, including strategic and operational, legal, financial, and reputational risks may also be prepared. The DPO should immediately consult with the CEO for breaches that have been identified as medium or high risk and those that are more likely to have a high impact on the College's strategic, operational, legal, financial, or reputational aspects.

Step 4: Notification

Under Article 33 GDPR, the college must report a data breach, if deemed reportable, to the Data Protection Commission within 72 hours of becoming aware of the breach. This timeframe includes weekends and bank holidays. If the relevant details surrounding the data breach are not clear within the initial 72-hour notification period, an initial notification should be made to the Data Protection Commission. Subsequent notifications can be made to the Data Protection Commission in phases. Consideration as to whether communication to affected individuals is required should be addressed when notifying the Data Protection Commission. All contact with the Data Protection Commission should be made through the DPO. If a decision is made to not report a breach, a summary record of the incident with an explanation of the basis for not informing the Data Protection Commission will be retained by the DPO.

Under Article 34 GDPR UniHaven must inform affected individuals without undue delay if the data breach is likely to result in a high risk to their privacy. Where the DPO assesses that there

is a high risk to the rights and freedoms of individuals because of the data breach, then the existence of the data breach should be communicated to the affected individuals without undue delay. Any such communication should inform the affected individuals of relevant measures that they can take to reduce the risks to them and any negative consequences arising from the data breach. The DPO should determine the most appropriate and effective means of communicating the data breach to the affected individuals, if necessary, engaging the CEO to establish how best to deal with the communications issues that have emerged. Notification should have a clear purpose, e.g., to enable individuals who may have been affected to take steps to protect themselves (e.g., by cancelling a credit card or changing a password), to allow regulatory bodies to perform their functions, provide advice and deal with complaints, etc. In each case, the notification should include as a minimum:

- A description of the nature of the breach.
- A description of the likely consequences of the breach.
- How and when the breach occurred.
- What data was involved?
- A description of the measures taken or proposed to be taken by the College to address the breach.
- The name and contact details of the DPO and other contact points.

The DPO in conjunction with the CEO should consider, and seek advice as appropriate, as to whether there are any other relevant notification requirements required (such as to the Gardaí, insurers, external legal advisers etc.).

Step 5: Evaluation & response

Certain data breaches will require further detailed investigation after the initial investigation period, which may involve external IT, legal and other support, as appropriate to ascertain the full extent of the data breach, its causes, and likely consequences and to effectively contain the breach. The effect of the data breach must be monitored, and the risks re-evaluated throughout this period. It may be necessary to agree to a phased notification program with the Data Protection Commission in these instances.

Step 6. Learning lessons

In the aftermath of a data breach, a post-incident review of the incident should take place to ensure that the steps taken during the incident were appropriate and effective, and to identify any areas that may be improved in future, such as updating policies and procedures or addressing systematic issues if they arise, to reduce the recurrence of similar data breaches and to ensure that appropriate technical and organisational security measures are put in place. A Breach Follow-Up Action Plan for data breaches and near misses should be completed and will form part of the investigation process. The action plan should clearly outline the lessons learnt, the controls agreed to reduce the risk of a further reoccurrence, a lead member of staff and a completion date. The case will not be considered closed until all actions agreed upon have been completed.

5. Quality Control

The Academic Director is responsible for ensuring that policies are developed and maintained, that they remain fit for purpose, that they remain in compliance with QQI guidelines, that they are updated as per agreed schedules, and that they are being implemented as intended. In the latter context, the Academic Director will inspect a sample of policies each year to check for the correct implementation and bring the findings to AC as part of the annual QA/QQI review and reporting process.

APPENDIX

UFORM022 Personal Data Breach Report Form Rev 1

Please act promptly to report any data security breaches. If you discover a data security breach, please notify your line manager immediately. Line managers need to complete Section 1 of this form and email it to the DPO at dpo@unihaven.ie.

Section 1: Notification of Data Security Breach	**To be completed by the Line Manager of the person reporting the incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting the incident:	
Contact details of the person reporting the incident (email address, telephone number, etc.):	
Brief description of the incident or details of the information lost:	
The number of Data Subjects affected if known:	
Has any personal data been placed at risk? If, so please provide details	
Brief description of any action taken at the time of discovery:	
For college use	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by DPO in consultation with the Line Manager affected by the breach.
Details of the IT systems, equipment, devices, and records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the college or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements e.g., to student sponsors?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH-RISK personal data o **Sensitive personal data** (as defined in the Data Protection Acts) relating to a living, identifiable individual's a) racial or ethnic origin. b) political opinions or religious or philosophical beliefs. c) membership of a trade union. d) physical or mental health or condition or sexual life. e) commission or alleged commission of any offence. f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
o Information that could be used to commit identity fraud such as personal bank	

account and other financial information and national identifiers, such as Personal Public Service Numbers (PPSNs) and copies of passports and visas.	
○ Personal information relating to vulnerable adults and children.	
○ Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed.	
○ Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
○ Security information that would compromise the safety of individuals if disclosed.	
Category of the incident (Lo Risk, Risk, Hi Risk):	
Reported to CEO:	
If Risk or Hi Risk, date escalated by DPO to the CEO/Executive Management Team	
Signature: _____	**Date:** _____

Quality Assurance Manual (QAM) Chapter 9	
Document Name	**Data Security Breach and Reporting Procedure**
Procedure Document Number	**UPRO013**
Version Reference	**Rev.1**
Document Owner	**Academic Director**
Roles with Aligned Responsibility	**Data Protection Officer, CEO**
Approved By	**Academic Council (AC)**
Approval Date	**3.2.2023**
Date Policy Becomes Active	**1.4.2023**
Revision Cycle	**Annually**
Revision History/Amalgamation History	**Revised for text errors post programme validation**
Additional Information	**N/A**
References/ Supporting Documentation	**UDOC000 UniHaven Quality Assurance Manual Rev 2** **Statutory Quality Assurance Guidelines developed by QQI for use by all Providers (2016)** **Statutory Quality Assurance Guidelines developed by QQI for Independent/Private Providers coming to QQI on a Voluntary Basis (2016)** **The Data Protection Acts 1988 and 2003 (as amended)** **Data Protection Legislation including Article 5 guidelines on (GDPR) General Privacy Data Regulations** **UPOL020 UniHaven Data Protection Policy Rev 1** **UPOL023 UniHaven Data Retention Policy Rev 1** **UPOL024 UniHaven Data Security Policy Rev 1** **UPOL025 UniHaven Learning Analytics Policy Rev 1** **A Guide for Data Controllers – Data Protection Commissioner** **Data Protection Regulation 2018** **https://www.dataprotection.ie/docs/GDPR/1623.htm** **European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. No. 336 of 2011)** **Data Protection Commissioner (www.dataprotection.ie)** **A Guide for Data Controllers (Office of the Data Protection Commissioner)** **http://www.dataprotection.ie/docs/a_guide_for_data_contollers/696.htm** **Personal Data Security Breach Code of Practice (29 July 2011)** **http://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm**