Data Retention Policy

1. Policy Overview

From the 25th of May 2018, the General Data Protection Regulation (the GDPR) impose obligations on the College, as a Data Controller, to retain the data for no longer than is necessary to achieve those purposes. This policy outlines the College's policy to comply with the GDPR requirements for data retention and data destruction.

2. Policy Statement

This policy is written in line with data protection requirements as outlined below and in line with QQI requirements that call for the use of nominated data retention periods[1].

Under GDPR, individuals have a right to be informed about how their personal data is processed, used, stored, and destroyed. The GDPR sets out the information that the College should supply to individuals and when individuals should be informed of this information. The College is obliged to provide individuals with information on data retention periods or criteria used to determine the retention periods and this policy has been written to set out the College's approach in these contexts. Under principle 7 of Data Protection Law, the College will only retain personal data for as long as needed and under any other legislative requirements on retention of such records. Should data need to be retained for research or similar purposes, it will be fully anonymised before being retained.

The College will take steps to destroy personal data records securely as they become redundant. At a minimum, there will be an annual review by business units of data that may

[1] Statutory Quality Assurance Guidelines developed by QQI for use by all Providers (2016), section 8.6

now be destroyed (as per the Retention Schedule in the Appendix), and action will be taken accordingly. UPOL020 UniHaven Data Protection Policy Rev 1 outlines the different types of data and provides the College's overarching approach to data protection. This policy should be read in tandem with it.

3. Roles and Responsibilities

Our Data Protection Officer, in conjunction with our Executive Management Team (EMT), is responsible for implementing this policy but all staff must comply with data protection requirements generally for the benefit of students, staff and stakeholders from whom we collect, process, and retain personal data. 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 timetables, 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.

4. Policy

Grounds for processing

Under the GDPR, the College is required to provide data subjects with the legal grounds or lawful basis that they are relying on for processing personal data. The legal grounds for processing personal data are as follows:

- Consent.
- Performance of a contract.
- Legal obligation.
- Vital interest.
- Public interest.
- Legitimate interests.

The above grounds are explained in more detail in UPOL020 UniHaven Data Protection Policy. If there is no justification for retaining personal information, then that information should be routinely deleted.

Further Retention and Processing Consent

Information should never be kept just in case a use can be found for it in the future. If the College wants to retain any personal data to help it to improve in any aspect, it must obtain consent from the relevant data subject for further processing and retention. Further retention of the personal data should be lawful only when it is compatible with the purposes for which it was originally collected. In this case, no separate legal basis is required - it should be relied on where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

Right of erasure

Individuals have the right to have their personal data erased and no longer processed in the following circumstances:

- Where the personal data is no longer necessary concerning the purposes for which they are collected or otherwise processed.
- Where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her.
- Where the processing of his or her personal data does not otherwise comply with the GDPR.
- Where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data,

especially on the internet. The data subject should be able to exercise that right even though he or she is no longer a child.

Retention Requirements

The College is required to retain certain records, usually for a specific amount of time. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences:

- Fines and penalties.
- Loss of rights.
- Obstruction of justice charges.
- Contempt of court charges.
- Serious disadvantages in litigation.
- Certain records must be retained because they contain information that:
    - Have enduring College value (for example, they provide a record of a commercial transaction, evidence the College's rights or obligations, protect its legal interests or ensures operational continuity.
    - Satisfies legal, accounting, or other regulatory requirements.

The College must balance these requirements with its statutory obligation to only keep records for the period required and to comply with data protection principles. The retention schedule in the Appendix sets out the relevant periods for the retention of College data and documents.

Types of Data

The different types of data to include records, disposable information, personal data, and confidential information belonging to others is outlined.

Records

A record is any type of information created, received or transmitted in the transaction of the College day-to-day running, regardless of physical format. Examples of where the various types of information are located are:

- Timetables and calendars.
- Tutorial or other learning support recordings.
- Computer programs.
- Contracts.
- Electronic files.
- E-mails.
- Handwritten notes.
- Invoices.
- Letters and other correspondence.
- Memory in mobile phones and PDAs.
- Online postings, such as on Facebook, Twitter, Instagram, LinkedIn, and other sites.
- Performance reviews.
- Voicemails.

Any paper records and electronic files that are part of any of the categories listed in the Records Retention Schedule contained in the Appendix must be retained for the respective periods indicated. A record must not be retained beyond the period indicated in the Record Retention Schedule unless a valid College reason (or a litigation hold or other special situation) calls for its continued retention or in cases where further consent for processing and retention has been secured from the relevant data subjects. Contact the Data Protection Officer should further clarification be needed on a case-by-case basis by emailing dpo@unihaven.ie.

Disposable Information

Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this policy. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of items such as but not limited to letters, memoranda, reports, timetables, correspondence, programme content, assessment strategies and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, learning and development material, and other printed materials obtained from sources outside of the College and retained primarily for reference purposes.
- Spam and junk mail.

Personal Data

Personal Data is defined as any data which can identify an individual either on its own or when combined with other data which we possess. Some examples of personal data include names and addresses, email addresses. See further information on personal data in UPOL020 UniHaven Data Protection Policy Rev 1 .

Confidential Information Belonging to Others

Any confidential information that a staff member may have obtained from a source outside of the College must not, so long as such information remains confidential, be disclosed to, or used by the College. Unsolicited confidential information submitted to the College should be refused, returned to the sender where possible and deleted.

The role of the Data Protection Officer in Data Retention

The responsibilities of the Data Protection Officer include advising the Academic Director about:

- Arranging for the proper storage and retrieval of records, coordinating with outside vendors where appropriate.
- Handling the destruction of records whose retention period has expired.
- Planning, developing and prescribing document disposal policies, systems, standards, and procedures.
- Monitoring departmental compliance so that management and staff know how to follow the document management procedures.
- Developing and implementing measures to ensure that it is clear what the College is retaining and where it is stored, that only authorised users to have access to the information, and that the College only retains the information it needs.
- Identifying essential records and establishing a disaster plan for each office and department to ensure maximum availability of UniHaven' records to re-establish operations quickly and with minimal interruption and expense.
- Determining if the College's document management program and its Records Retention Schedule follows the relevant legislation.
- Ensuring that the maintenance, preservation, storage, and destruction of College records is carried out under this policy and in line with QQI requirements for information management.

5. Procedures and Forms

UPRO012 UniHaven Data Subject Access Request Procedure Rev 1 and UPRO013 UniHaven Data Security Breach and Reporting Procedure Rev 1 complement this policy. The procedure for records disposal as outlined below.

Record Disposal Procedure

The College acknowledges its duty to dispose of records securely and this will be done as follows:

- When hard copy records are to be destroyed as per the Retention Schedule in the Appendix, this should be done by a GDPR-compliant shredding provider and records of such destruction kept for larger volumes or by College staff using the College own office shredders for smaller volumes.
- When I.T. equipment becomes redundant, all storage devices associated with that equipment must be securely destroyed by a GDPR-compliant computer equipment destruction provider so that any data on the storage device may no longer be retrieved. The contracting organisation should also sign off to certify that the records were destroyed.
- Data that is stored in electronic form and then destroyed should have any backup copies of it destroyed simultaneously. When the original data is destroyed, any backups that are not destroyed with it become the only copy and become subject to the Data Regulations Acts' full requirements. The contracting organisation should also sign off to certify that the records were destroyed.
- When records are destroyed, a register of destruction should be kept in perpetuity so that there is always a back reference to what records were disposed of and when. Where personal data is destroyed, the date of the destruction event should be captured for each record, along with the procedure that was used, the person who oversaw the destruction, their department, by whom the authority was given to destroy the records, and the data subject's name, contact details, and any other relevant information that identifies them.

Appendix

Record Retention Schedule

The College has outlined its retention periods for specific categories of records. Staff should give special consideration to the categories of documents listed in the record retention schedule below. Avoid retaining a record if there is no College reason for doing so and consult with the Data Protection Officer if unsure.

1. College-wide Records

Owner	General class of Records held	Default retention period	Final Disposition
1.1. General Administrative Records			
CEO	Strategic Plans	Retained no longer than is necessary for the purposes for which it was processed	Appropriate filing/archiving
CEO	Records of Board of Directors, EMT, Academic Council and related committees, e.g., agenda, minutes, documents relating to agenda items i.e., reports etc.	Retained no longer than is necessary for the purposes for which it was processed	Appropriate filing/archiving
CEO	Institute organisational structure	Retain current until superseded	Appropriate filing/archiving
Academic Director	Quality Assurance Manual, and associated policies, procedures, forms, manuals, and handbooks	Retain current for 3 years or less if superseded	Confidential shredding/secure deletion of electronic records
Academic Director/ Programme Manager	Records of committees, e.g., agenda, minutes, documents relating to agenda items i.e., reports etc.	Retain for 5 years, or until actions are completed	Confidential shredding/secure deletion of electronic records
CEO, Academic Director	Institute risk register, local risk registers	Retain for 5 years after superseded	Confidential shredding/secure deletion of electronic records

Owner	General class of Records held	Default retention period	Final Disposition
CEO	Projections and statistical analysis	Retain for current plus 6 years	Confidential shredding/secure deletion of electronic records
Chair of Meeting	Handwritten notes taken by recording secretary present at meetings	Retain until minutes have been agreed and signed by Chair at following meeting of the committee	Destroy confidentially as appropriate.
All	General (non-HR) written allegations/complaints; records received/created because of investigating allegations/complaints	Retain for 5 years after resolution of complaint from date of last correspondence	Confidential shredding/secure deletion of electronic records
All	Routine administration records	Retain for current year, or until they cease to be of administrative use.	Appraise and evaluate for secure archiving where relevant otherwise, confidential shredding/secure deletion of electronic records
All	General correspondence, including emails	Retain for current year, or until they cease to be of administrative use	Appraise and evaluate for secure archiving where relevant otherwise, confidential shredding/secure deletion of electronic records

Owner	General class of Records held	Default retention period	Final Disposition
1.2. Other Administration Records			
Programme Manager	Teaching allocations/timetables	Retained no longer than is necessary for the purposes for which **it** was processed	Appraise and evaluate for secure archiving where relevant otherwise, confidential shredding/secure deletion of electronic records
All	General correspondence including emails	Retain for current year, or until they have ceased to be of administrative use	Appraise and evaluate for secure archiving where relevant otherwise, confidential shredding/ secure deletion of electronic records
Academic Director	Annual Quality Reports, QQI reviews, QQI Revalidation, Programme Annual Reports, Programme Development, Programme Accreditation	Retain for 5 years	Confidential shredding/secure deletion of electronic records

Owner	General class of Records held	Default retention period	Final Disposition
1.3. Legal Records			
CEO	Legal cases, advice, and correspondence	Retain for 5 years after resolution of complaint from date of last correspondence	Appropriate filing/archiving
CEO	Copyright, business registration documents	Retain indefinitely	Appropriate filing/archiving
Academic Director	Contracts for services, maintenance contracts	Retained no longer than is necessary for the purposes for which it was processed	Appropriate filing/archiving
Chief Revenue Officer	Commercial contracts	Retained no longer than is necessary for the purposes for which it was processed	Appropriate filing/archiving
Academic Director	Leases and rental agreements	Retained no longer than is necessary for the purposes for which it was processed	Appropriate filing/archiving

2. Student Records

Owner	General classes of records held	Default retention period	Final Disposition
2.1. Applications and Applicants			
Academic Director	Records of successful applicants	Retain for duration of studies plus 5 years	Confidential shredding/secure deletion of electronic records
Academic Director	Records of unsuccessful applicants where no appeal was initiated	Retain for no longer than two years. Anonymised applicant data may be retained for as long as required for administrative or statistical use.	Confidential shredding/secure deletion of electronic records.
Academic Director	Unsuccessful applicant appeals submissions, appeal committee reports/outcomes	Retain for 5 years following completion of action	Confidential shredding/secure deletion of electronic records.
Academic Director	Collaboration agreements including agents	Retain for duration of agreement plus 2 years	Confidential shredding/secure deletion of electronic records.

Owner	General classes of records held	Default retention period	Final Disposition
2.2. Enrolled Students			
Programme Manager	Student registration record (incl. student name, ID number, contact details on LMS etc.)	Retain for duration of studies plus 3 years	Appropriate filing/archiving
Programme Manager	Records including leave of absences, deferral, transfer, readmission, exemptions, student status etc.	Retain for duration of studies plus 3 years	Confidential shredding/secure deletion of electronic records
Programme Manager	Attendance forms and extenuating circumstances forms	Retain for 12 months after the end of the programme in the academic year to which they apply.	Confidential shredding/secure deletion of electronic records
Programme Manager	College correspondence with students	Retain for duration of studies plus 3 years	Confidential shredding/secure deletion of electronic records
Programme Manager	Records of student awards/scholarships, prizes	Retained no longer than is necessary for the purposes for which it was processed	Appropriate filing/securing, archiving.
Academic Director	Student discipline records	Retain for 5 years following completion of action	Confidential shredding/secure deletion of electronic records
CEO	Student fees/financial: Records re student fees, payment records, bank transfers	Retain for duration of studies plus 3 years	Confidential shredding/secure deletion of electronic records

Owner	General classes of records held	Default retention period	Final Disposition
2.3. Examinations, results, graduation records			
Programme Manager	Examination papers (and related records i.e., recommended marking scheme, suggested solutions etc. where relevant, grade appeals/rechecks/reviews., scripts, coursework)	Retain for duration of studies plus 3 years	Appropriate filing/securing archiving
Programme Manager	Final year projects and associate records, raw data etc. Other records including raw data to be retained within relevant department.	Retain for 3 years following deadline for appeal	Confidential shredding/secure deletion of electronic records
Academic Director	External Examiner Reports	Retain for a minimum of current year plus 3 years (until no longer required)	Appraise and evaluate for archiving where relevant otherwise, confidential shredding/secure deletion of electronic records
Academic Director	External examiner correspondence, meetings, records etc.	Retain for current year plus 3 years	Confidential shredding/secure deletion of electronic records
Academic Director	Records of module grades	Retain for duration of studies plus 3 years	Appropriate filing/secure archiving
Academic Director	Amendment to marks, published results/grade alteration correspondence	Retain for duration of studies plus 3 years	Appropriate filing/secure archiving
Academic Director	Formal broadsheets	Retain for duration of studies plus 3 years	Appropriate filing/secure archiving
Academic Director	Examination board meeting records	Retain for duration of studies plus 3 years	Appropriate filing/secure archiving
Programme Manager	Student academic transcript	Retain for duration of studies plus 3 years	Appropriate filing/secure archiving
Academic Director	Student data post-graduation	Retain for duration of studies plus 3 years	Appropriate filing/secure archiving

3. Financial Records

Owner	General classes of records held	Default retention period	Final disposition
CEO	Accounts Payable, e.g., invoices, VAT	Retain for current year plus 7 years plus additional time if required by contract or policy or agreement	Confidential shredding/secure deletion of electronic records
CEO	Accounts Receivable, e.g., reconciliations, aged debtors, creditors, bank details		
CEO	Annual financial statements		
CEO	Final budget reports		
CEO	Registers – i.e., Risk register, IT Register, Fixed Asset register		
CEO	Insurance records to include claims		
CEO	Rental, lease, use, occupancy		
CEO	Pay-sheets, authorisation to deduct tax details of staff, appointment details, pay scales		
CEO	Listings/payslips		

4. People Records

Owner	General class of records held	Default retention period	Final disposition
4.1. Recruitment/competition files/selection committees			
People Officer	Unsolicited applications for positions	None	Confidential shredding
People Officer	Vacancy notification Advert copies, job descriptions, selection criteria	Retain for current year plus 5 years plus additional time if required by consent	
People Officer	Candidates not qualified or shortlisted for interview: Cover letters, application forms/CV's etc.		
People Officer	Applications and CV's of candidates shortlisted for interview but who did not attend: Cover letters		
People Officer	Candidates shortlisted and who attend interview but who are not successful or who were successful but do not accept offer.		
People Officer	Interview board marking sheet Interview board notes Panel Recommendations by Selection Committees		

Owner	General class of records held	Default retention period	Final disposition
4.2. Staff Files			
People Officer	May include such records such as: • Staff contact and ID details • Application form/CV/cover letter • Contract of employment (offer of appointment, date appointed) • Evidence of education qualifications • References • Occupational health assessment • Probation forms • Salary • Termination notices • Learning and development records • Training records • Leave	Retain on personnel file for duration of employment and for 5 years after last salary payment or as per policy or contract or settlement if higher	Confidential shredding/secure deletion of electronic files.
People Officer	Records relating to disciplinary actions taken against employees HR allegations and complaints Written allegations/complaints Records received/created because of investigating allegations/complaints External employee relations claims, awards, settlements		

Owner	General class of records held	Default retention period	Final disposition
4.4. Occupational Health Records, Health and Safety			
CEO	Incident reports e.g., Accident reports and dangerous occurrence reports	Retain for 7 years after date of incident.	Confidential shredding/secure deletion of electronic files.
CEO	Occupational health reports not relating to specific members of staff	Retain for 7 years after date of incident.	Appropriate filing/secure archiving and confidential shredding/secure deletion of electronic files
CEO	Safety audits, investigations, and safety evaluation records where cases result in significant changes to policy	No longer than is necessary for the purposes for which **it** was processed	Appropriate filing/secure archiving.
CEO	Notifications of personal accidents or hazardous situations on campus (which result in injuries/compensation claims)	Please refer to "insurance" section	

5. Marketing Records

Owner	General class of records held	Default retention period	Final Disposition
5.0. Public Affairs and Communications			
CRO	College press releases	No longer than is necessary for the purposes for which it was processed	Appropriate filing/secure archiving.
CRO	PR Campaigns	No longer than is necessary for the purposes for which it was processed	Appropriate filing/secure archiving.
CRO	Formal records of ceremonies/functions, e.g., honorary conferring's VIP visits, photographs, audio-visual recordings, programmes of events as relevant	No longer than is necessary for the purposes for which it was processed	Appropriate filing/secure archiving.
CRO	Social media campaigns	No longer than is necessary for the purposes for which it was processed	Appropriate filing/secure archiving.

Quality Assurance Manual (QAM) Chapter 9	
Document Name	**Data Retention Policy**
Procedure Document Number	**UPOL023**
Version Reference	**Rev.1**
Document Owner	**Academic Director**
Roles with Aligned Responsibility	**All staff, DPO**
Approved By	**Academic Council (AC)**
Approval Date	**2.3.2023**
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 Retention Policy** **UPOL024 UniHaven Data Security Policy** **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**