Data Security Policy

1. Policy Overview

This policy sets out the College approach to securing staff, student, and stakeholder data.

2. Policy Statement

This policy is written in line with data protection requirements as referred to below and in line with QQI requirements where providers are expected to "*establish quality assurance procedures to support the management and integrity of learner results data which provides the basis for making and certifying QQI awards. Voluntary providers must also have procedures for the maintenance of records in this regard*[1]."

The Data Protection Acts 1988 and 2003 (as amended) (the DPA) and, from the 25th of May 2018, the General Data Protection Regulation (the GDPR) impose obligations on the College, as a Data Controller, to secure data in a manner that assures those who have provided personal data that this data is being held securely. To this end, this policy should be read in tandem with UPOL020 UniHaven Data Protection Policy Rev 1. See also UPOL025 Learning Analytics Policy Rev 1 and UPOL023 UniHaven Data Retention Policy Rev 1 for detail on the type of student data that the College collects and stores.

3. Roles and Responsibilities

The Data Protection Officer, in conjunction with our Executive Management Team (EMT), is responsible for securing data in the College, and for briefing, all staff in their responsibilities

[1] Statutory Quality Assurance Guidelines developed by QQI for Independent/Private Providers coming to QQI on a Voluntary Basis (2016), section 8.

to students and stakeholders on what needs to be done to maintain the integrity of the College data security approaches.

4. Policy

As per UPOL020 UniHaven Data Protection Policy Rev 1and UPOL023 UniHaven Data Retention Policy Rev 1, the College will request, process and store different types of personal data for specified purposes that have been provided by applicants, students, parents, and stakeholders. Personal data should be secured according to the below guidelines:

- Paper – all personal data should be stored in lockable drawers and cabinets that are only accessible by the staff responsible for processing it and the Line Manager of those staff. No personal records or other data should be left visible or lying about on top of desks, cabinets, or other open surfaces. Where possible, all sensitive personal data should be scanned into a soft copy format and stored on the company servers with the original copies shredded.
- Electronic mail – all email is automatically protected by the College's back-end security software programmes, namely ESET Endpoint security, firewall and antivirus protection.
- Electronic files and folders are only to be stored on the company servers that are protected by the College's back-end security software programmes, namely ESET Endpoint security, firewall and antivirus protection. Folders have been set up with pre-authorised permissions to ensure that staff only access information on a "need-to-know" basis.
- All data submitted <u>to the College</u> by electronic transfer, be it email, electronic money transfer, and other online forms of data transfer is the responsibility of the data provider and/or a third-party data controller or data processor to secure and protect until the point at which the College receives it. Such third-party data processors or controllers that the College employs will have signed written contracts with the College that will have had data protection-compliant clauses included.
- All data submitted <u>by the College</u> by electronic transfer, be it email, electronic money transfer, and other online forms of data transfer is the responsibility of the College staff

to transfer in a data-secure manner. All data transfers facilitated through third parties shall only be done by reputable third-party providers that the College has written signed agreements with. Such third-party data processors or controllers will have signed written contracts with the College that will have had data protection-compliant clauses included.

- All files and email are backed up automatically through Office 365 via Ek.co Backup for Microsoft 365.

5. Procedures and Forms

UPRO013 UniHaven Data Security Breach and Reporting Procedure Rev 1should be read in conjunction with this policy. It explains how data security breaches are managed, reported, and generally dealt with.

Quality Assurance Manual (QAM) Chapter 9	
Document Name	**Data Security Policy**
Procedure Document Number	**UPOL024**
Version Reference	**Rev.1**
Document Owner	**Academic Director**
Academic Director	**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**