Data Protection Policy

1. Policy Overview

This policy outlines the College's policy on data protection so that it complies with relevant GDPR legislation.

2. Policy Statement

The College is committed to protecting individuals' rights and privacy under QQI requirements as follows[1]:

- Reliable information and data are available for informed decision-making and to ensure the providers know what is working well and what needs attention.
- Controls and structures are in place to generate named data/reports which are communicated to staff and management for self-monitoring and planning purposes.
- The information gathered reflects the context and mission of the provider.

The College also seeks to comply with relevant data protection legislation, especially the Data Protection Act 2018. This bill

- Entitled an Act to establish a body to be known as the Data Protection Commission.
- To give further effect to Regulation (E.U.) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and the free movement of such data, and repealing Directive 95/46/E.C. (General Data Protection Regulation).
- To give effect to Directive (E.U.) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data by competent authorities for the purposes of the prevention, investigation,

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

detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

- To give further effect to the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data done at Strasbourg on the 28th day of January 1981 and for those and other purposes to amend the Data Protection Act 1988.
- To provide for the consequential amendment of certain other enactments; and to provide for related matters.

Data Protection is how individuals' privacy rights are safeguarded concerning their personal data processing. The College needs to collect and use personal data about its students, staff, and other individuals that it deals with as an international College. Those individuals ("data subjects") have privacy rights about the processing of their personal data. The College must, therefore, comply with the E.U. General Data Protection Regulation ("GDPR") and the Irish Data Protection Acts, 1988 to 2018 (the "DPA") – known collectively in this policy as "the Data Protection Acts". The Data Protection Acts confer rights on individuals as well as responsibilities on those who process personal data. This policy applies to all College centres should it open more than one teaching centre in the future.

This data protection policy sets out, in writing, how personal data on staff, students and other individuals (e.g., parents, stakeholders etc.) is kept and how the data concerned is protected. Personal data is subject to certain legal safeguards specified in the Data Protection Act 2018. The Act imposes restrictions on how that data may be used. The policy sets out the rules on data protection and the legal conditions that must be satisfied concerning the obtaining, handling, processing, storage, transportation, and destruction of personal data. This policy outlines College responsibilities in this regard and refers to those other policies and procedures which deal with specific aspects of data protection. It will be reviewed regularly in light of any legislative or other relevant indicators and amended as needed.

Relevant definitions

- **Data:** means information in a form that can be processed. It includes automated data (information on a computer or information recorded to put it on a computer) and manual data (data that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system).
- **Collection** (of information) is the gathering, acquiring, or obtaining from any source and by any means including, without limitation:
    - Verbally.
    - By letter or other written form.
    - Electronically via a computer screen or email.
    - By videotape or other electronic media.
- **Relevant filing system** means any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals so that specific information relating to a particular individual is readily accessible.
- **Personal data** means data relating to a living individual who is or can be identified from the data or from the data in conjunction with other information that is in or is likely to come into, the possession of the data controller.
- **Data controllers** are organisations or people who control and are responsible for the personal data which they hold. They determine the purposes for which and how any personal data is processed. They have a responsibility to establish practices and policies in line with data protection legislation. The College is the data controller of all personal data.
- **Joint data controller** is where two or more parties may properly exercise legal or de facto control and responsibility for a given set of personal data. This situation is rare.
- **Data processors** include any organisations or people who process personal data on behalf of a data controller. The staff of data controllers are excluded from this definition, but it could include suppliers which handle personal data on behalf of the College.

One company or person can be both a data controller and a data processor in respect of distinct sets of personal data. For example, a payroll company would be the data controller in respect of the data about its staff but would be the data processor in respect of the payroll data it is processing for the staff of its client companies.

To collect and process personal data "lawfully", the College must have a legal basis for doing so. There are six available legal bases for processing. No single basis is better or more important than the others – which basis is most appropriate to use will depend on the purpose and the relationship with the individual. The six legal bases set out in Article 6(1) of the GDPR are as follows:

Processing shall be lawful only if and to the extent that at least one of the following applies:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering a contract.
- Processing is necessary for compliance with a legal obligation to which the controller is subject.
- Processing is necessary to protect the vital interests of the data subject or another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller.
- Processing is necessary for the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The College must determine its legal basis before beginning to process personal data and should document it in its data protection notifications. In cases where the College relies on consent as a condition for processing personal data, it must:

- Obtain the data subject's specific, informed and freely given consent.
- Ensure that the data subject gives consent by a statement or an explicit affirmative action.
- Document that statement/affirmative action.
- Allow data subjects to withdraw their consent at any time without detriment to their interests.

- **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in the possession of a Data Controller). Personal data can be factual (such as a name, address, or date of birth), or it can be an opinion (such as a performance review).
- **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, bio-metric to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

  In the case of personal data relating to special categories of data, it is necessary for the processing to be covered both by a legal basis and by a special category condition set out in Article 9 of the GDPR. In the case of personal data relating to criminal convictions and offences, it is necessary for the processing to be covered both by a legal basis and by a separate condition for processing this data in compliance with Article 10 of the GDPR. Both types of processing need to be documented to demonstrate accountability and compliance.

- **Health Information** is a subset of sensitive personal data and includes a person's:
  - Health or disability (past, present, or future).
- **Processing** is any activity that involves the use of the data. It includes obtaining, recording, or holding the data or carrying out any operation or set of operations on the data, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

- **Text messaging, or texting**, is the Act of composing and sending brief, electronic messages between two or more mobile phones or fixed or portable devices over a phone network.
- **Use** means how information is used within an organisation.

3. Roles and Responsibilities

While the owner of this policy is the Data Protection Officer, all staff have a role to play in protecting staff and student data, particularly academic staff, and admissions staff, and to treat all personal data with great care. 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

Records

The following types of data are collected and stored as records at the College:

- Staff records may be kept in manual record/filing system and electronic format/filing system to facilitate the payment of staff for salaries and leave, learning and development, role changes, grievance, and disciplinary matters etc. and include:
    - Name, address and contact details, PPS number.
    - Original records of application and appointment.
    - Record of appointments to roles.
    - Details of approved absences (annual leave, career breaks, parental leave, study leave etc.).
    - Details of work record (qualifications, classes taught, subjects etc.).
    - Details of complaints and/or grievances, including consultations or competency discussions, action/improvement/evaluation plans, and progress records.

  Note: A record of grievances may be maintained, which is distinct from and separate to individual staff files.

- Student records may be kept in manual record/filing system and electronic format/filing system to enable each student to develop his/her full potential, to comply with legislative or administrative requirements, to ensure that eligible students can benefit from the relevant additional teaching or financial supports, to support the provision of information regarding visa applications to study in Ireland or overseas, to enable parent/guardians to be contacted in the case of emergency, to progress students to Higher Education Institution (HEI) partners etc.:
    - The information that may be sought and recorded at enrolment includes:
        - Name, address and contact details, passport number.
        - Names and addresses of parents/guardians and their contact details.
        - Education transcripts/proof of record.
        - Racial, ethnic, or national origin.

        - Any student disabilities or conditions that may impede their learning at the College…see UPOL018 UniHaven Learner Disability Policy Rev 1 for the way such information is sought and processed and used.
    - Language assessments.
    - Attendance Records.
    - Academic record – subjects studied, class assessments, and examination results as recorded on official College records.
    - Records of significant achievement.
    - Records of disciplinary issues and/or sanctions imposed.
    - Recordings of online delivered tutorials for making available to students to replay for the benefit of their learning.
    - Other records, e.g., records of any serious injuries/accidents etc.

- Meeting records may be kept in manual record/filing system and electronic format/filing system as a record of member details, minutes of meetings, appointments, documenting decisions made by the relevant board, committee, or council etc. that may include:
    - Name, address, and contact details of each member attending.
    - Records concerning appointments to the meeting body.
    - Minutes of the meetings and correspondence to the meeting body may include references to particular individuals, be they staff, students or external individuals.

Conditions for Processing Special Categories of Personal Data

The GDPR sets out conditions for processing Special Categories of personal data. The college must satisfy a lawful condition of personal processing data under Article 6 of the GDPR as well as one under Article 9 to process these categories of data.

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.
- Processing is necessary for carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement under Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
- The processing relates to personal data, which are manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Processing is necessary for reasons of substantial public interest, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- Processing is necessary for preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services based on Union or Member State law or under contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and medicinal products or medical devices, based on Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular, professional secrecy.
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes under Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- Personal data may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or regulations established by national competent bodies.

Note: There will be several additional grounds for processing special categories of personal data (such as health data) under Irish law, in addition to those contained in Article 9 of the GDPR. Notably, these include a legal basis to process health data for insurance, pension or mortgage purposes which, for the College, is limited to its need to collect medical information relating to any students who present with sickness, illness, injury, disabilities or conditions that may impede their learning and where a staff member needs to complete an occupational health assessment to gauge their fitness for fulfilling their employment role.

Conditions for Processing Personal Data About Criminal Convictions or Offences (Article 10)

The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings, or convictions. Instead, there are separate safeguards for personal

data relating to criminal convictions and offences or related security measures set out in Article 10. To process personal data about criminal convictions or offences, the College must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10. You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this. The Data Protection Bill deals with this type of data in a similar way to special category data and sets out specific conditions providing lawful authority for processing it. Article 10 also specifies that the College can only keep a comprehensive register of criminal convictions if it is doing so under the official authority's control.

Details of arrangements in place to ensure compliance with the eight rules of data protection

The policy outlines the arrangements in place to ensure that all personal data records held by the College are obtained, processed, used, and retained under the following eight rules of data protection (based on the Data Protection Acts):

- Obtain and process information fairly and lawfully.
- Keep it only for one or more specified, explicit, and lawful purposes.
- Use and disclose it only in ways compatible with these purposes.
- Keep it safe and secure.
- Keep it accurate, complete, and up to date.
- Ensure that it is adequate, relevant, and not excessive.
- Retain it for no longer than is necessary for the purpose or purposes.
- Give a copy of his/her personal data to that individual on request.

And, also:

- Not to transfer personal data to people or organisations without adequate protection.

Obtain and process information fairly and lawfully

Procedures have been put in place to ensure that staff members, parents/guardians and students are made fully aware when they provide personal information of the identity of the persons who are collecting it, the purpose in collecting the data, the persons or categories of persons to whom the data may be disclosed and any other information which is necessary so that processing may be fair. The College will process personal data fairly and under the fulfilment of its functions. This includes informing the data subject of the purpose of collecting their data and anyone to whom the data may be disclosed or transferred. Information obtained from a third party (e.g., a relative or guardian) is governed by the same confidentiality rules as if it were obtained directly.

Obtaining information fairly and lawfully also includes obtaining their consent to obtaining and processing their personal data (unless unable to do so, in which case its use must be to prevent injury or other damage to their health). Article 7 of the GDPR outlines the conditions for consent as follows:

- Where the processing is based on consent, the College must be able to demonstrate that the data subject has consented to the processing of his or her personal data.
- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner that is distinguishable from the other matters, in an intelligible and easily accessible form using clear and plain language. Any part of such a declaration that constitutes an infringement of the regulation shall not be binding.
- The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Before giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
- When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

<u>Lawful Basis for Processing (Article 6)</u>

It is necessary under Article 6 of the GDPR to have a legal basis for processing ALL personal data. There are six legal bases set out in the legislation:

- Consent from the individual
    - The individual must give consent at the outset. Inferred consent is not enough. Their consent must be freely given, and the withdrawal of their consent should not have any adverse consequences for the individual.

- Necessary for the performance of a contract
    - The contract must be between the controller and the data subject. The data must be necessary for the performance of that contract or necessary to take steps to enter a contract with the data subject. For example, processing data relating to an individual's qualifications and work history when considering entering into an employment contract, students' academic history and qualifications when they apply to study at the College etc.
- Necessary for compliance with a legal obligation
    - The College is required by statute to retain certain records, for example, employment records, health & safety records.
- Necessary to protect the vital interests of the individual or another natural person
    - This ground is applied in essentially "life and death" situations, for example, where it is necessary to provide personal data to the emergency services in the case of an emergency.
- Necessary for the performance of a task carried out in the public interest
    - This may occur where the College carries out a task in the public interest or in an exercise where official authority has been invested in the College as a data controller. However, a data subject can object to this lawful basis and challenge whether the processing is indeed in the public interest.
- Necessary for the legitimate interests of the controller or a third party
    - The processing is necessary for the College legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests and in the case of special categories of personal data, as covered by one of the lawful bases as set out in Article 9(1) of the GDPR, for example:
        - Explicit consent from the individual.
            - Necessary for legal obligations of the controller as an employer insofar as it is authorised by E.U. or Irish law.

  - Necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent.
- Data has been 'manifestly made public by the data subject themselves.
  - Necessary for medical or health reasons subject to any applicable DPA measures and safeguards.
  - Necessary for the public interest' subject to any applicable DPA measures and safeguards.

In the case of personal data relating to criminal convictions and offences, it must be covered by a lawful basis as set out in the DPA.

Keep it only for one or more specified, explicit, and lawful purposes

- Those whose data is collected by the College are informed in advance about the reason/s why it is collected and kept.
- The purpose for which the data is collected and kept is lawful.
- Staff are aware of the different sets of data that are kept, and the specific purpose of each.

Use and disclose it only in ways compatible with these purposes.

The College_will only process personal data for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the legislation. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

- Data is used only in ways consistent with the purpose/s for which it was obtained.
- Data is disclosed only in ways consistent with that purpose.

- Procedures are in place, which is following the Data Protection Acts, to facilitate the transfer of information to HEI partners when students wish to progress to them, and students will have given prior consent for this to occur.
- The College outlines the circumstances in which it will disclose personal data to third parties to data subjects before the disclosure taking place.
- Procedures are in place under the Data Protection Acts to facilitate the transfer of personal data abroad as international transfers
- Exceptions to disclosure rule:
    - Data can be disclosed when required by law.
    - Data can generally be disclosed to an individual himself/herself or with his/her consent.
- Refer to UPOL009 UniHaven Staff Recruitment and Selection Policy Rev 1 for the data collected at the recruitment and selection stage including occupational health assessments.

<u>Keep it safe and secure.</u>

The College will take appropriate security measures against unlawful or unauthorised personal data processing and the accidental loss of, or damage to, personal data. It is aware that high standards of security are essential for all personal data. Personal data may only be transferred to a third-party data processor if that data processor agrees to comply with our procedures and policies or puts in place adequate measures themselves. The College commits that

- Appropriate security measures have been taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.
- Access to the information (including the authority to add/amend/delete records) is restricted to authorised staff on a "need to know" basis.
- Has detailed who has access to what information based on this “need to know” policy… see UPOL023 UniHaven Data Retention Policy Rev 1.

- All IT and computer systems will be password protected and centrally managed by the College IT provider.
- Information on computer screens and manual files will be kept out of view of callers to College offices.
- Automatic backup procedures are in operation for computer held data, including off-site back-ups… see UPOL024 UniHaven Data Security Policy Rev 1.
- All reasonable measures have been taken to ensure that staff know the security measures at induction and comply with them.
- All waste papers, printouts etc. are disposed of carefully, including the shredding of confidential information in College office shredders. Any bulk shredding of old files will only be done via a registered shredding company that can certify destruction…see UPOL023 UniHaven Data Retention Policy Rev 1.
- Steps have been taken to ensure that no unauthorised person can access data from computers no longer in use or subject to change of use as recorded on the College IT register.
- A contract IT company has been designated to be responsible for the security of all IT servers and systems. Third-party IT providers are contractually responsible for the security of their systems and GDPR compliance as either data controllers and/or processors.
- Reviews of the measures and practices in place take place annually via EMT.
- Premises will be secured by lock, key, and alarm when unoccupied.

Keep it accurate, complete, and up to date.

Personal data must be accurate and kept up to date. All information that is incorrect or misleading is not valid. The College will maintain procedures to ensure high data accuracy levels, including checking data at the time of recording, correct any errors when advised or discovered, and regular audits of records.

- Clerical and computer procedures are adequate to ensure high levels of data accuracy.

- Appropriate procedures in place, including periodic review and audit, to ensure that each data item is kept up to date.

Ensure that it is adequate, relevant, and not excessive for the purpose

Personal data will only be collected to the extent required for the specific purpose of the data subject. Any data which is not necessary for that purpose will not be collected in the first place. The College ensures that data is held as per UPOL023 UniHaven Data Retention Policy Rev 1and that it

- Is held adequate concerning the purpose/s for which it is kept.
- It is held relevant concerning the purpose/s for which it is kept.
- Is held not excessive concerning the purpose/s for which it is kept.

Retain it for no longer than is necessary for the purpose or purposes

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased when it is no longer required. The College policy for retention periods for personal data and procedures for disposal are outlined in UPOL023 UniHaven Data Retention Policy Rev 1. Retention times cannot be rigidly prescribed to cover every possible situation. The College has exercised its judgement in this regard concerning each category of records held.

Where litigation may potentially arise in the future (e.g. about accidents/personal injuries involving staff, students or for accidents occurring on College property, the relevant records should be retained until the probability of litigation eases. The statute of limitations concerning personal injuries is currently two years. The limitation period for other causes of action varies, but in most cases is not greater than six years. A limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim. In the case of minors, the limitation period does not begin to run until they reach their 18th birthday or later if the date of knowledge postdates their 18th birthday.

Give a copy of his/her personal data to an individual, on request and in line with the data subject's rights

The College will maintain procedures to ensure that data subjects can exercise their rights to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

To make an access request, an individual must refer to UPRO025 UniHaven Data Subject Access Request Procedure Rev 1, apply in writing and give any details which might be needed to help identify him/her and locate all the information that the College may keep about him/her.

Do not transfer personal data to people or organisations situated in countries without adequate protection

The College will not transfer personal data to people or organisations in countries without adequate protection. All College agreements will have data protection elements to them and, where possible, will be subject to Irish or European data protection laws. The minimum age at which consent can be legitimately obtained for processing and disclosure of personal data is not defined in the Data Protection Acts. However, guidance material published on the Data Protection Commissioner's website states the following:

"As a general rule in the area of education, a student aged eighteen or older may give consent themselves. A student aged from twelve up to and including seventeen should give consent themselves and, in addition, consent should also be obtained from the student's parent or guardian. In the case of students under the age of twelve, consent of a parent or guardian will suffice.". Refer also to UPOL017 UniHaven QQI Student Support Policy Rev 1 for the College's guardian nominee services to students who are minors.

Transfers to Third Countries (Outside the European Economic Area)

Flows of personal data to and from the European Union (the "E.U.") are necessary for international trade and international cooperation. However, the transfer of such personal data from the E.U. to controllers and processors located outside the E.U. in third countries should not undermine the level of protection of the individuals concerned, with a third country being any country outside the European Economic Area (the "EEA"). Therefore, transfers to third countries or international organisations should be done in full compliance with Chapter V of the General Data Protection Regulation, the "GDPR". Any staff member who proposes to transfer data outside of the EEA should first consult with the DPO to ensure suitable arrangements are made and necessary contracts and or agreements are put in place in line with this policy.

The first thing to consider when transferring personal data to a third country is if there is an "adequacy decision". An adequacy decision means that the European Commission has decided that a third country or an international organisation ensures an adequate data protection level. When assessing the adequacy of the level of protection, the European Commission considers elements such as the laws, respect for human rights and freedoms, national security, data protection rules, the existence of a data protection authority and binding commitments entered into by the country in respect of data protection.

The adoption of an adequacy decision involves:

- A proposal from the European Commission;
- An opinion of the European Data Protection Board ("EDPB");
- an approval from representatives of E.U. countries; and
- The adoption of the decision by the European Commissioners.

The effect of such a decision is that personal data can flow from the EEA to that third country without any further safeguard being necessary. In other words, the transfer is the same as if it was carried out within the E.U. A list of countries with an adequacy decision is Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, United States of America (limited to the Privacy Shield framework – this is no longer available since July 2020) as providing adequate protection.

In the absence of an adequacy decision, the GDPR does allow a transfer if the controller or processor has provided "appropriate safeguards". These safeguards may include:

- Standard data protection clauses: For most organisations, the most relevant alternative legal basis to an adequacy decision would be these clauses. They are model data protection clauses that the European Commission has approved and enable the free flow of personal data when embedded in a contract. The clauses contain contractual

obligations on the Data Exporter and the Data Importer and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the Data Importer and the Data Exporter. These are known as the 'standard contractual clauses'. There are two sets of standard contractual clauses for restricted transfers between a controller and a controller and one set between a controller and a processor. The European Commission has advised the EDPB that it plans to update the existing standard contractual clauses for the GDPR. Until then, EU-based data controllers can still enter contracts that include the standard contractual clauses based on the E.U. Directive 95/46/E.C., which pre-dated the GDPR.

- Binding corporate rules "BCRs": BCRs form a legally binding internal code of conduct operating within a multinational group, which applies to transfers of personal data from the group's EEA entities to the group's non-EEA entities. This group may be a corporate group, or a group of undertakings engaged in a joint economic activity, such as franchises or joint ventures. BCRs are legally binding data protection rules with enforceable data subject rights contained in them, which the competent Data Protection Authority approves. Two types of BCRs can be approved - BCR for Controllers which are used by the group entity to transfer data that they have responsibility for, such as employee or supplier data, and BCR for Processors which are used by entities acting as processors for other controllers and are normally added as an addendum to the Service Level Agreement or Processor contract. Further provisions on the use of BCRs as an appropriate safeguard for personal data transfers are set out in GDPR Article 47.
- Approved Codes of Conduct: The use of Codes of Conduct as a transfer tool, under specific circumstances, has been introduced by the GDPR in Article 40 (3). Codes are voluntary and set out specific data protection rules for categories of controllers and processors. They can be a useful and effective accountability tool, providing a detailed description of the most appropriate, legal, and ethical behaviour within a sector. From a data protection viewpoint, codes can therefore operate as a rulebook for controllers and processors who design and implement GDPR-compliant data processing activities that give operational meaning to the principles of data protection set out in European

and national law. Codes of Conduct that relate to personal data processing activities by controllers and processors in more than one E.U. Member State, and for which the E.U. Commission has adopted an implementing act, together with binding and enforceable commitments of the controller or processor in the third country, could be used as a transfer tool in the future. The EDPB is planning to issue separate specific guidance related to the use of Codes of Conduct as a transfer tool later.

- Approved certification mechanisms: The ISO defines certification *as "the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements"*. Therefore, as introduced in the GDPR in Article 42 (2), certification mechanisms may be developed to demonstrate the existence of appropriate safeguards provided by controllers and processors in third countries. These controllers and processors would also make binding and enforceable commitments to apply the safeguards, including data subject rights provisions. The EDPB is also planning to issue separate specific guidance on using certification mechanisms as a transfer tool.
- A legally binding and enforceable instrument between public authorities or bodies: An organisation can make a restricted transfer if it is a public authority or body and is transferring to another public authority or body and with both public authorities have signed a contract or another instrument that is legally binding and enforceable (Article 46 (2)(a) GDPR). This contract or instrument must include enforceable rights and effective remedies for individuals whose personal data is transferred. This is not an appropriate safeguard if either the transferring organisation or the receiver is a private body or an individual. If a public authority or body does not have the power to enter legally binding and enforceable arrangements, it may consider an administrative arrangement that includes enforceable and effective individual rights instead (Article 46 (3)(b) GDPR). The EDPB is currently working on updated guidance about these transfer tools.

Article 49 – Derogations for specific situations

Derogations under Article 49 are exemptions from the general principle that personal data may only be transferred to a third country if an adequate level of protection is provided for in that third country. A Data Exporter should first endeavour to frame transfers with one of the mechanisms guaranteeing adequate safeguards listed above and only in their absence use the derogations provided in Article 49 (1). These derogations or exceptions allow transfers in specific situations, such as based on consent, for the performance or conclusion of a contract, for the exercise of legal claims, to protect the vital interests of the data subject where they cannot give consent or for important reasons of public interest. The EDPB guidance document on these derogations should always be consulted to ensure that they could be relied upon for the specific scenarios that organisations are dealing with issues.

5. Procedures and Forms

The College Data Protection Impact Assessment Procedure outlines how to risk assess new proposals/projects in a data protection context while the below procedures outline procedures for data subject access requests and data security breach reporting with relevant forms included in each.

- UPRO025 UniHaven Data Subject Access Request Procedure Rev 1
- UPRO026 UniHaven Data Security Breach and Reporting Procedure Rev 1

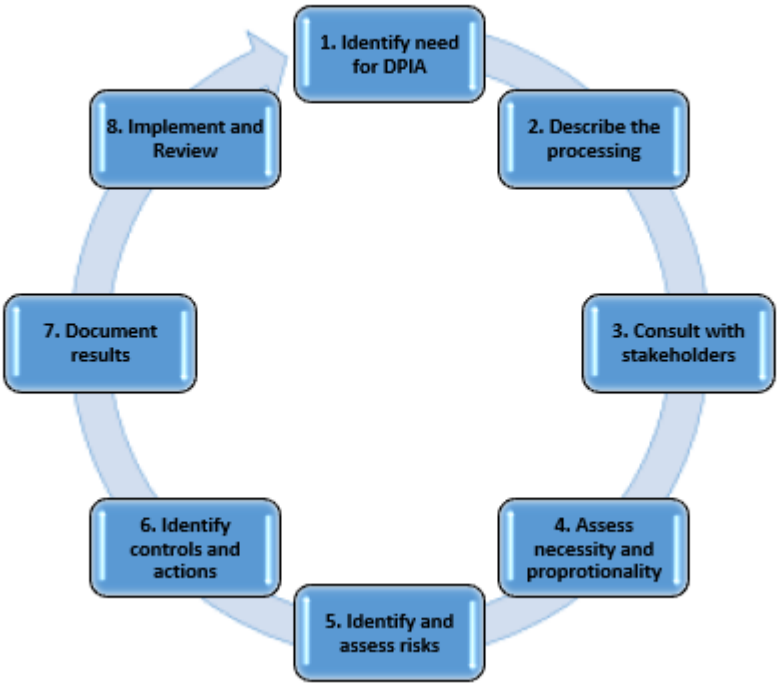
Appendix

Data Protection Impact Assessment Procedure

A Data Protection Impact Assessment (DPIA) is a process to help to identify and minimise the data protection risks of a project. It facilitates the systematic and comprehensive analysis of data processing to identify and minimise data protection risks. It is an important tool for building and demonstrating compliance with the GDPR (i.e., accountability). Under the General Data Protection Regulation (GDPR), the College must carry out a DPIA where a planned or existing processing operation is "likely to result in a high risk" to individuals. Although GDPR provides examples of data processing that would fall into this category, this is a non-exhaustive list. It is also good practice to do a DPIA for any other major project that requires personal data processing. The purpose of this procedure is to enable the College to identify when a DPIA is mandatory and how to carry out a DPIA.

All new projects and significant changes to existing systems/processes which require the processing of personal data must perform at least step 1 of this procedure to determine if a full DPIA is required. DPIAs should consider compliance risks but also broader risks to the rights and freedoms of data subjects, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or society at large, whether it is physical, material or non-material. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. A DPIA does not have to eradicate the risks but should help to minimise risks and assess whether or not the remaining risks are justified.

The DPIA Procedure



Step 1: Identify the Need for a DPIA/whether a DPIA is mandatory

The GDPR does not require a DPIA to be carried out for every processing operation, which may result in risks for the rights and freedoms of natural persons. The carrying out of a DPIA is only mandatory where personal data processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35 GDPR). The GDPR provides (a non-exhaustive list of) some examples of processing that would fall into this category. The following should be taken into account when determining if the processing is high risk and therefore requiring a DPIA or not.

You must do a DPIA if you plan to carry out one or more of the following:

1. Evaluation and scoring (including profiling and predicting), especially concerning a data subject's performance at work, economic situation, health, personal preferences, reliability or behaviour, location, or movements. An example would be gathering social media profile data to generate profiles for contact directories or marketing.

2. Automated decision-making with legal or similarly significant effects **-** Is a decision made by automated means without any human involvement? An example would be deciding who is selected for an interview based on a recruitment aptitude test that uses pre-programmed algorithms and criteria.
3. Systematic monitoring - including through a publicly accessible place on a large scale. For example, using a camera to monitor driving behaviours on a road.
4. Sensitive data or data of highly personal nature – this includes special categories of data as defined in Article 9:
    - Racial or ethnic origin.
    - Political opinions.
    - Religious or philosophical beliefs.
    - Trade union membership.
    - Data concerning health.
    - Data concerning a person's sex life or sexual orientation.
    - Genetic data.
    - Biometric data.
    - As well as criminal data as defined in Article 10. An example would be a hospital keeping patient medical records or an organisation keeping an offender's details.
5. Data processed on a large scale – while the term 'large scale' is not defined, the regulators recommend the following is taken into account: (a) the number of data subjects concerned; (b) the volume and range of data been processed; (c) the duration and permanence of the processing; (d) the geographic extent of the processing activity.
6. Datasets have been matched or combined – for example, two or more data processing operations performed for different purposes and/or by different data controllers been combined in a way that would exceed the reasonable expectation of the data subject.
7. Data concerning vulnerable data subjects – For example, children are considered unable to oppose or consent to the processing of personal data knowingly. Asylum seekers would be considered vulnerable data subjects.

8. Innovative use or applying technological or organisational solutions – for example, combining the use of fingerprint and face recognition for improved physical access control.
9. When processing prevents the data subject from exercising a right or using a service or a contract – for example, processing a public area that people passing cannot avoid or processing that aims to refuse data subjects access to a service or contract (bank screens its customers against a credit reference database to decide whether to offer a loan).

In cases where it is not clear if a DPIA should be carried out, the regulators' guidance is that a DPIA should be carried out as it is a useful tool to comply with GDPR. Advice on whether a DPIA should be carried out can be sought from DPO.

Step 2: Describe the Processing in a Systematic Way

Describe how and why you plan to use the personal data. Your description must include "the nature, scope, context and purposes of the processing".

The nature of the processing is what is planned to be done with the personal data. This must include:

- How you collect the data is collected.
- How you store the data is stored.
- How you use the data is used.
- Who has access to the data?
- With whom is the data shared.
- Whether any processors are used.
- Retention periods.
- Security measures.
- Whether you are using any new technologies are being used.
- Whether you are using any novel types of processing are being used
- Which screening criteria have been identified as likely high risk.

The scope of the processing is what the processing covers. This must include:

- The nature of the personal data.
- The volume and variety of the personal data.
- The sensitivity of the personal data.
- The extent and frequency of the processing.
- The duration of the processing.
- The number of data subjects involved.
- The geographical area covered.

The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact. This might include, for example:

- The source of the data.
- The nature of your relationship with the individuals.
- The extent to which individuals have control over their data.
- The extent to which individuals are likely to expect the processing.
- Whether they include children or other vulnerable people.
- Any previous experience of this type of processing.
- Any relevant advances in technology or security.
- Any current issues of public concern.
- Whether you have considered and complied with relevant codes of practice.

The purpose of the processing is the reason why you want to process the personal data. This must include:

- Tour legitimate interests, where relevant.
- The intended outcome for individuals.
- The expected benefits for you or society.

Step 3: Assess Necessity and Proportionality

You should consider:

- Do your plans help to achieve your purpose?
- Is there any other reasonable way to achieve the same result?
- The lawful basis for the processing.
- How you will prevent function creep, i.e., using the data for more than the original purpose.
- How you intend to ensure data quality.
- How you intend to ensure data minimisation.
- How you intend to provide privacy information to individuals.
- How you implement and support individual's rights.
- Measures to ensure your processors comply.
- Safeguards for international transfers.

Step 4: Consult with Stakeholders

The views of data subjects (or their representatives) should be sought unless there is a good reason not to. In most cases, it should be possible to consult individuals in some form. External stakeholders could include people who will be affected by the project and members of the public. However, it is decided that it is not appropriate to consult individuals, then this decision should be recorded as part of the DPIA with a clear explanation. Suppose the DPIA covers the processing of personal data of existing contacts (for example, existing students or staff). In that case, a consultation process to seek those individuals or their representatives' views should be designed.

If the DPIA covers a plan to collect the personal data of individuals that have not yet been identified, there may be a need to carry out a more public consultation process or targeted research. This could take the form of carrying out market research with a certain demographic

or contacting relevant campaign or consumer groups for their views. If the DPIA decision is at odds with the views of individuals, there is a need to document the reasons for disregarding their views. If a data processor is used, there may be a need to ask them for information and assistance.

Step 5: Identify and Assess Risks

Identify the potential risks that may arise. Consider the potential impact on individuals and any harm or damage that might be caused by the processing – whether physical, emotional or material. Look at whether the processing could contribute to:

- Inability to exercise rights (including but not limited to privacy rights).
- Inability to access services or opportunities.
- Loss of control over the use of personal data.
- discrimination.
- Identity theft or fraud.
- Financial loss.
- Reputational damage.
- Physical harm.
- Loss of confidentiality.
- Re-identification of pseudonymised data.
- Any other significant economic or social disadvantage.

An assessment of the security risks should be included, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data). Having identified the risks, it is then necessary to assess which are going to pose the greatest threat by looking at both the likelihood of the risk occurring and the impact that might result. This provides the overall risk rating.

Step 6: Identify Controls and Actions

Against each risk identified, consider options for reducing that risk. Identify the current controls (how is risk currently managed) and what further actions will be taken to reduce the impact/likelihood and mitigate the risk. For example, some actions and controls that could be implemented are:

- Deciding not to collect certain types of data.
- Reducing the scope of the processing.
- Reducing retention periods.
- Taking additional technological security measures.
- Training staff to ensure risks are anticipated and managed.
- Anonymising or pseudonymising data where possible.
- Writing internal guidance or processes to avoid risks.
- Adding a human element to review automated decisions.
- Using a different technology.
- Putting clear data-sharing agreements into place.
- Making changes to privacy notices.
- Offering individuals the chance to opt-out where appropriate;
- Implementing new systems to help individuals to exercise their rights.

Step 7: Document Results

Record:

- What additional measures you plan to take.
- Whether each risk has been eliminated, reduced, or accepted.
- The overall level of residual risk after taking additional measures.
- Whether the Data Protection Commission needs to be consulted.

Risk does not always need to be eliminated. Some risks, and even high risk, are acceptable given the benefits of the processing and the difficulties of mitigation. Record all reasons for

choosing a particular approach and any reasons for going against the views of individuals or other consultees.

Step 8: Implement and Review

Integrate the outcomes of the DPIA back into the project plans. Identify any action points and who is responsible for implementing them. Monitor the ongoing performance of the DPIA. There may be a need to cycle through the process again before plans are finalised. If a high risk has been accepted, either because it is not possible to mitigate or because the mitigation costs are too high, there is a need to consult the Data Commissioner before proceeding.

Quality Assurance Manual (QAM) Chapter 9	
Document Name	**Data Protection Policy**
Procedure Document Number	**UPOL020**
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** **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** **UPOL021 UniHaven Privacy Policy Rev 1** **UPOL022 UniHaven Cookie Policy Rev 1** **UPOL023 UniHaven Data Retention Policy Rev 1** **UPOL024 UniHaven Data Security Policy Rev 1**