Data Protection Policy

Policy Name – Data Protection Policy	
Version number: 4	
Policy Owner	**Policy Author/Reviewer**
Chief People Officer	Office of the University Secretary
Approving body	**Date of approval**
Approved by SLT	14 November 2023
	Equality Screened
	Yes
	Next Review date
	November 2028
Queries relating to this document should be directed to the Policy Owner – Eoin Coyle, gdpr@ulster.ac.uk. This document can be made available on request, in alternative formats and in minority languages to meet the needs of those who are not fluent in English.	

ULSTER UNIVERSITY

DATA PROTECTION POLICY

1. INTRODUCTION

As an academic institution, Ulster University (the **University**) processes a range of Personal Data in the discharge of its duties as an educational intuition and employer. Such Personal Data must only be processed by the University in accordance with the Data Protection legislation.

This Data Protection Policy sets out how the University processes the Personal Data entrusted to it by prospective, current and former students and University staff, alumni, research participants and suppliers. University staff and students that process Personal Data on behalf of the University must comply with this policy at all times.

The University is committed to protecting the data rights of individuals and recognises its legal obligation to ensure the correct and lawful treatment of Personal Data. Such legal obligations are taken seriously by the University as is the integrity of Personal Data. This Data Protection Policy sets out how the University manages its responsibilities in this regard.

In this Data Protection Policy, references to “we” “our” and “us” shall mean the University and references to “you” shall mean University staff and students that process Personal Data on the University’s behalf. You will find a glossary of the terms used within this Data Protection Policy at Appendix 1. This Data Protection Policy should be read together with the Related Policies listed at Appendix 2.

The University’s Data Protection Officer (DPO) is responsible for overseeing this Data Protection Policy.

The position, independence and responsibility of the DPO is defined in Article 39 of UK GDPR to:

- Inform and advise the University and its employees about their obligations under Data Protection legislation.
- Monitor compliance with the UK GDPR.
- Advise on Data Protection Impact Assessments (DPIAs).
- Raise awareness of Data Protection legislation.
- Co-operate with the supervisory authority, the Information Commissioner’s Office, and act as its contact point.
- Contact point for the administration of all Data Subject Rights relating to data held by the University; and
- Ensure University policy, guidelines and security measures are appropriate and up to date for the types of data being processed.

1. AIMS OF THE DATA PROTECTION POLICY

The aims of this Data Protection Policy are:

- to identify the roles and responsibilities of University staff in respect of compliance with this Data Protection Policy;
- to make University staff and students that process personal data on the University's behalf aware of the University's legal obligations under the Data Protection legislation;
- to set out the University's strategy for ensuring compliance with the Data Protection legislation in respect of processing Personal Data entrusted to the University;
- to minimise the risk to the University of any potential breach of the Data Protection legislation;
- to ensure all individuals (Data Subjects) are aware of their rights under the Data Protection legislation; and
- to encourage valued relationships with stakeholders and trust in the University's handling of Personal Data.

2. SCOPE

This Data Protection Policy shall apply to all Personal Data that the University processes and applies equally to information held in hardcopy or electronic form, which shall include photographic material and CCTV footage. This Data Protection Policy shall apply regardless of the party that created the Personal Data, where it is held, or the ownership of the equipment used.

3. DATA PROTECTION PRINCIPLES

All processing of Personal Data that you complete on behalf of the University must comply with the seven Data Protection principles contained within the UK GDPR. In summary, the Data Protection principles require that Personal Data is:

(i) processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency)**;
(ii) collected only for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes **(Purpose Limitation)**;
(iii) adequate, relevant and limited to what is necessary in relation to the purpose(s) for which it is processed **(Data Minimisation)**;
(iv) accurate and kept up to date **(Accuracy)**;
(v) not kept in a form which permits identification of individuals for longer than is necessary for the purpose(s) it is processed **(Storage Limitation)**;
(vi) Processed in a way ensures its security and to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage **(Integrity and Confidentiality);** and
(vii) responsible for demonstrating compliance with the above listed principles (**Accountability**).

These seven Data Protection principles are the foundation on which the remainder of the legislation is built and so all University staff and students must be mindful to comply with these principles at all times when processing Personal Data.

4. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

In compliance with the first Data Protection principle set out above, Personal Data must be processed fairly, lawfully and in a transparent manner for specified purposes. UK GDPR requires that processing of Personal Data must be for one or more lawful purposes under Article 6 of UK GDPR, known as a "**lawful basis**".

At least one of the following "lawful bases" must apply whenever Personal Data is being processed:

(i) **Consent:** the individual (Data Subject) has provided their informed consent to process their Personal Data for a specific purpose;

(ii) **Contract:** the processing is necessary for a contract with the Data Subject or is required to take specific steps before entering into a contract with the Data Subject;

(iii) **Legal obligation:** the processing is necessary to comply with the law (not including contractual obligations);

(iv) **Vital interests:** the processing is necessary for the protection of the vital interests of the Data Subject or another person;

(v) **Public task:** the processing is necessary to perform a task in the public interest or for official functions; and

(vi) **Legitimate interests:** the processing is necessary for the legitimate interests of the party processing the Personal Data, unless there is a good reason to protect the Data Subject's Personal Data which overrides such legitimate interests. This lawful basis will not apply if a public authority (such as the University) is processing Personal Data to perform its public tasks.

You must identify the appropriate lawful basis **before** you commence to process any Personal Data on behalf of the University and **keep a record** of the lawful basis which is being relied upon. Further information which may help you identify the appropriate lawful basis appears within the University Data Protection Guidance.

5. CONSENT

In the event University is relying upon consent as its lawful basis, you should be aware that UK GDPR sets a high standard for consent and that a number of requirements will need to be established before you can lawfully rely upon consent.

Consent may not be the most appropriate lawful basis to rely upon and other lawful bases may be more easily satisfied. For these reasons, you should consider if there is another lawful basis available before seeking to rely upon consent. For further guidance please contact gdpr@ulster.ac.uk.

6. TRANSPARENCY (PRIVACY NOTICES)

Further to the transparency principle, the Data Protection Legislation requires that the University informs Data Subjects how their Personal Data is used by the University in a detailed, specific and easily accessible manner. Such information must be included within a privacy notice. A template notice is available for staff.

A number of the University's privacy notices meanwhile are available online at: https://www.ulster.ac.uk/about/governance/gdpr.

You should ensure that the privacy notice issued by you or your department complies with the ICO requirements, as further described within the University Data Protection Guidance. A copy

of the Privacy Notice must be supplied to the Data Protection & Information Compliance Unit by sending to GDPR@ulster.ac.uk.

7. PURPOSE LIMITATION

To comply with the purpose limitation principle, all Personal Data must be collected for a **specified, explicit and legitimate purpose** and cannot be further processed in a way that is incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed to the Data Subject, unless you have informed the Data Subject of the new purposes and they have consented where necessary.

8. DATA MINIMISATION

Personal Data collected and otherwise processed by the University must comply with the data minimisation principle and should be **relevant and limited** to what is necessary in relation to the purposes it is processed.

Accordingly, you should be mindful of ensuring any Personal Data you collect on behalf of the University is limited to what is necessary and is not excessive. Once the Personal Data is no longer needed for the identified purpose, you should ensure that it is deleted in accordance with the University's Records Retention and Disposal Schedule.

9. ACCURACY

Pursuant to the accuracy principle, all Personal Data held by the University must be accurate and, where applicable, updated. It should be corrected or deleted as soon as possible when the University is notified that it is inaccurate. As far as possible, you must ensure that the Personal Data we use and hold is **accurate, complete, up to date and relevant**.

10. STORAGE LIMITATION

To realise the storage limitation principle, Personal Data **must not be kept in an identifiable form for longer than is necessary** for the purposes for which the Personal Data was processed or as may be required by law. The University's Record Retention and Disposal Schedule and the Records Management Policy are maintained to ensure that Personal Data is deleted after an appropriate time in line with the storage limitation principle and the University's statutory obligations for legal and accounting reporting.

11. SECURITY INTEGRITY & CONFIDENTIALITY

In line with the principle of integrity and confidentiality, we must secure the Personal Data by using appropriate technical and organisational measures against unauthorised processing and against the accidental loss, destruction or damage of the Personal Data.

The University continually develops, implements and maintains safeguards appropriate to the size, scope, available resources, amount of Personal Data we maintain and the identified risks. Such safeguards include:

- making sure that, where appropriate, Personal Data is pseudonymised or encrypted;
- ensuring the integrity and resilience of our processing systems and services;
- ensuring that, in the event of a physical or technical incident, availability and access to Personal Data can be restored in a timely manner; and
- maintaining a process for regularly testing, assessing and evaluating the effectiveness of technical organisational measures to ensure the security of the processing.

You must follow all of our policies, procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You must also exercise particular care in protecting Special Category Data and Criminal Offence Data from accidental loss or disclosure.

Where the University engages a third party to process Personal Data on its behalf, or otherwise shares Personal Data with another party, additional security arrangements must be implemented into the relevant agreement to safeguard the security of the Personal Data.

12. ACCOUNTABILITY

The University must be in a position to establish how it has complied with the other Data Protection principles, pursuant to the accountability principle. The accountability requirements include the completion of DPIAs, reporting of Data Breaches and University staff training.

13. RECORD KEEPING

In accordance with our obligations under the Data Protection legislation, the University must keep written records of its processing activities. When you process Personal Data on behalf of the University, you must keep written records of such activities.

Please ensure all **details are reflected in your departmental Information Asset Register** so that our records can be kept up to date.

14. PERSONAL DATA BREACHES

The University is responsible for ensuring appropriate security for the Personal Data entrusted to it, which includes protecting Personal Data against unauthorised or unlawful processing and against accidental loss or destruction.

Actions Required in the Event of a Personal Data Breach

The University shall make every effort to avoid a Personal Data Breach from occurring, however if one should occur, the Data Protection legislation requires the University to notify the Information Commissioner's Office (ICO) without undue delay and no later than **72 hours** after having become aware of it. In some circumstances the University will also have to notify the Data Subject without undue delay.

Given the statutory reporting timeframes, we require you to:

- **submit a Personal Data Breach Report Form to the Data Protection Officer ('DPO') immediately upon discovery** of a Personal Data Breach or suspected breach;
- provide all factual information available within the Personal Data Breach Report Form;
- co-operate with the Data Protection & Information Compliance Unit with their investigations and response to all queries as a matter of urgency; and
- preserve all evidence relating to the suspected Personal Data Breach.

The Personal Data Breach Report Form and further details are available here. Once completed, immediately email the Report Form to gdpr@ulster.ac.uk. A member of staff from the Data Protection & Information Compliance Unit shall then contact you in confidence to discuss the content of the report.

The University shall investigate all incidents of a suspected or actual Personal Data Breach and take appropriate action to mitigate the consequences and prevent similar events occurring in the future. Should the investigation confirm that a Personal Data Breach has in fact occurred, the Data Protection & Information Compliance Unit shall notify the ICO, where required, notify the Data Subject and update the Data Breach Register accordingly.

What incidents should be reported to the University's DPO at gdpr@ulster.ac.uk

Any Personal Data Breach or suspected Personal Data Breach including but not limited to any incident that **could potentially compromise the security of Personal Data** such as:

- theft of a laptop;
- loss of mobile phones, flash drives and other data storage devices;
- sending an email or letter to the wrong address;
- loss of Personal Data resulting from an equipment or systems failure;
- loss of hardcopy documents are files which contain Personal Data;
- non arrival of sensitive information;
- maintenance of unsecured databases;
- human error, such as accidental deletion or alteration of Personal Data;
- unforeseen circumstances, such as a fire or flood; and
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams.

The above list is not exhaustive and should you be in in any doubt, please simply report the suspected incident to the DPO out of an abundance of caution.

15. RIGHTS OF DATA SUBJECTS

Data Subjects Rights

Under the Data Protection legislation, a Data Subject has the following rights, all of which are qualified in different ways:

(i) **The right to be informed:** a Data Subject has the right to be informed about the collection of their Personal Data and to be informed of how their Personal Data is being used by the University. This is a key transparency requirement under the UK GDPR.

(ii) **The right of access to your Personal Data:** a Data Subject has the right to request access to their Personal Data held by the University, which is known as a "**Subject Access Request**". A Subject Access Request does not have to be submitted in any particular format nor does the request have to include the phrase 'subject access request' or refer to Data Protection legislation.

(iii) **The right to rectification:** a Data Subject has the right to have inaccurate Personal Data held by the University rectified or completed if it is incomplete.

(iv) **The right to be forgotten:** a Data Subject has the right to have their Personal Data held by the University erased. This right is not absolute and only applies in certain circumstances as detailed in Article 17 of UK GDPR.

(v) **The right to restrict processing:** a Data Subject has the right to restrict processing of their Personal Data. This right is not absolute and only applies in certain circumstances as detailed in Article 18 of UK GDPR.

(vi) **The right to data portability:** a Data Subject has the right to receive copies of their Personal Data in a machine readable and commonly used format. This right is not absolute and only applies in certain circumstances as detailed in Article 20 of UK GDPR.

(vii) **The right to object:** a Data Subject has a right to object to the processing of their Personal Data. This right is not absolute and only applies in certain circumstances as detailed in Article 21 of UK GDPR.

(viii) **Rights in relation to automated decision making and profiling:** a Data Subject has a right not to be subject to a decision based solely on automated decision-making using their Personal Data without any human involvement. Profiling (Automated Processing of Personal Data to evaluate certain things about an individual) can be part of an Automated Decision-Making process. This right is not absolute and only applies in certain circumstances as detailed in Article 22 of UK GDPR.

Further information in respect of a Data Subject's rights is available from the ICO here.

Exercising Data Subject Rights

Any person who wishes to exercise any of those rights listed above, can make their request either verbally on telephone no. 028 701 24533 or by email to gdpr@ulster.ac.uk.

Should a member of University staff receive a request to exercise any of those rights listed above, they should immediately share the request with the DPO by emailing gdpr@ulster.ac.uk. It is important that **University staff can recognise a request to exercise an individual's rights** and in particular recognise a Subject Access Request so that they can share the request immediately with the DPO to allow the University to comply with the statutory timeframes for response.

Timeframes for Response

The University undertakes to consider and act upon a request without undue delay. In compliance with the Data Protection legislation, this will be at the latest **within one month** of receipt of a request. However, that period may be extended by 2 further months where necessary, taking into account the complexity and number of the requests. The University shall inform the Data Subject of any such extension within 1 month of the receipt of the request, together with the reasons for the delay.

Identity of Requester

The University will require photographic proof of identity prior to acting upon a request in every case. The University shall let the Data Subject know without undue delay and within one month

that it needs such additional information. The University does not need to act upon a request until it has received the additional information.

16. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Privacy By Design

Under the Data Protection legislation, the University is required to implement "privacy by design" measures to show that we have given consideration to our Personal Data processing activities from the outset. Privacy by design measures that can be implemented will be informed by and take account of the cost of implementing such measures, the nature of the processing and the risks to the rights of the Data Subject. To ensure implementation of privacy by design, the University are required to conduct DPIA's in certain circumstances.

When a DPIA is Required

The Data Protection legislation requires the University to conduct DPIAs in respect of **high risk processing**. The purpose of a DPIA is to help identify the Data Protection risks of a project so that appropriate mitigations can be put in place and assist with compliance with our obligations under the Data Protection legislation.

University staff should conduct a DPIA and discuss findings with the DPO when implementing a major system or business change programs involving the processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- automated processing including profiling and automated decision making;
- Processing of Special Category Data or Criminal Offence data;
- large-scale, systematic monitoring of a publicly accessible area; and

It is also good practice to conduct a DPIA for any other major project which requires the processing of Personal Data.

The University internal procedures and the template DPIA are available here. Completed DPIAs should be submitted to gdpr@ulster.ac.uk, for consideration and response by the GDPR team. You must not proceed with any proposed processing until a response has been received in respect of the submitted DPIA.

17. SPECIAL CATEGORY DATA & CRIMINAL OFFENCE DATA

Given its sensitivity, Special Category data and Criminal Offence data attract higher protections under the Data Protection legislation. There are **additional conditions** which must be satisfied before processing such Personal Data, which University staff and students processing data on the University's behalf, should be mindful of and consider carefully. For further information on how to ensure compliance when processing these types of Personal Data, please see the University Data Protection Guidance.

18. AUTOMATED PROCESSING AND AUTOMATED DECISION MAKING

Generally, Automated Decision Making is prohibited when a decision has a significant effect on an individual unless:

- the Data Subject has explicitly consented;
- the processing is authorised by law; or
- the processing is necessary for the performance of or entering into a contract.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects will be informed when the University first communicates with them of their right to object. This right must be **explicitly** brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

Should you expect to be involved in any Personal Data processing activity that involves profiling or Automated Decision Making, they must contact the DPO in advance.

19. RESPONSIBILITIES OF UNIVERSITY STAFF AND STUDENTS

Anyone who processes Personal Data for the University, be that University staff or students that process data on the University's behalf, are required to adhere to this Data Protection Policy and the Related Policies.

In summary, all University staff, students that process data on the University's behalf and other such processors commit to ensuring that they:

- Read and comply with this Data Protection Policy and the Related Policies, as may be updated from time to time;
- Seek advice from the DPO when unsure about how to comply with this Data Protection Policy and the Related Policies to ensure compliance with the Data Protection legislation;
- Ensure that all Personal Data is obtained for **specified**, **explicit** and **legitimate purpose** and is only processed for those purposes;
- Ensure that all Personal Data is processed **lawfully, fairly and transparently** with a "legal basis" for processing (see section 4 above);
- They only use the **minimum amount of Personal Data** necessary to fulfil the purpose and which is relevant to such purpose;
- **Do not disclose Personal Data to unauthorised persons**, whether within or outside the University and at all times ensure access is restricted to authorised persons;
- Keep and store the Personal Data **securely** with the level of security appropriate to the sensitivity of the Personal Data and in accordance with the University Records Management Policy;
- Ensure that the use of, and access to, computers, laptops and other portable electronic data processing/storage devices are compliant with University guidance contained within the Code of Practice for Use of Ulster University Computer Networks, Equipment and Telephone Systems;
- **Only retain** the Personal Data for **as long as strictly necessary** to fulfil the purpose of its processing and in accordance with Records Retention and Disposal Policy;
- Ensure the Personal Data provided to the University are **accurate** and where applicable notify the University immediately of any changes or errors so that the record can be updated or erased as appropriate;
- Immediately report any suspected Personal Data Breaches in accordance with section 14 above and follow all recommended next steps as advised by the DPO;
- Inform University security staff immediately of incidents where persons without proper authorisation are found in areas where Personal Data is held or processed; and

- Avoid disclosing Personal Data by telephone unless you are certain the caller is the person they claim to be, and is authorised to receive the Personal Data in question.

In addition, all University staff must also:

- Complete the compulsory Data Protection training programme together with any further training as specified by the University from time to time;
- Promptly respond to any requests from the University Data Protection Team in connection with any Subject Access Requests, Data Subject rights based requests or complaints and immediately forward any such requests if received directly to the University Data Protection & Information Compliance Unit so that we can comply with the statutory timeframe for response;
- Where University staff are responsible for supervising students involved in work which requires the processing of Personal Data, they University staff are required to ensure that the students are fully aware of the Data Protection principles, the requirements of this Data Protection Policy and Related Policies and the need to obtain the informed consent of any Data Subjects involved as appropriate; and
- Avoid, in so far as possible, recording personal opinions not based on fact about a Data Subject. These comments will be disclosable.

20. TRAINING

The University shall ensure that training is made available to University Staff regarding their Data Protection responsibilities. You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy.

The University shall maintain a record of training attendance by University staff.

21. CONSEQUENCES OF FAILING TO COMPLY

The University takes compliance with this Data Protection Policy and the Related Policies very seriously given failure to comply:

- puts at **risk the individuals** whose Personal Data is being processed;
- carries the risk of significant **civil and criminal sanctions** for the individual and the University;
- could result in **the ICO exercising its powers** against the University, which include information notices, enforcement notices, inspection powers or fines, which can be up to **£17.5million or 4% or global annual turnover**, whichever higher; and
- expose the University to **reputational damage**.

Because of the importance of this Data Protection Policy and the Related Policies, any alleged breach of same by University staff or students processing on the University's behalf shall be fully investigated. Such investigations may lead to disciplinary action and in some instances may be considered gross misconduct and result in dismissal (where applicable).

22. SHARING PERSONAL DATA

Generally the University is not permitted to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

Internal Sharing

University staff can only share the Personal Data with another staff member, agent or representative of the University if the recipient has a job-related **need to know** the Personal Data.

External Sharing

University staff may only share the Personal Data entrusted to the University with third parties, such as its service providers or other public bodies, if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross-border transfer restrictions; and
- a data sharing agreement has been entered. To note, the University has a range of data sharing agreements which address the range of relationships that may arise which are available upon request to gdpr@ulster.ac.uk.

We have also prepared a data sharing checklist available [Your Guide to Data Protection], which you should consult in advance of proceeding to transfer Personal Data with an external third party.

23. INTERNATIONAL / CROSS BORDER TRANSFERS

There are **restrictions** imposed on the University by UK GDPR when transferring Personal Data outside the UK (a "restricted transfer") to ensure the same level of protection is afforded to individuals' Personal Data. The University is permitted to make restricted transfers so long as they comply with certain conditions, namely:

(i) where the UK have approved the recipient country as having adequate data protection laws and procedures (known as an "**adequacy regulation**"); or

(ii) where the University have put in place certain **safeguards** in accordance with the Data Protection Legislation, which will typically take the form of entering an approved form data sharing agreement called the **International Data Transfer Agreement;** or

(iii) there is an **exemption** available so that the University can proceed with the Restricted Transfer in absence of (i) or (ii) above, albeit such exemptions are narrow and won't apply to circumstances where the University is pursuing its public task of teaching and research.

Most frequently, the University will proceed to make a restricted transfers in reliance of adequacy regulations.

Should you receive a request to transfer Personal Data to a country that does not have an adequacy regulation, the University and the recipient will most likely need to enter the International Data Transfer Agreement to ensure the transfer is compliant.

24. DIRECT MARKETING

The University is subject to certain rules and privacy laws when distributing marketing materials to contacts under the Privacy and Electronic Communications Regulations and UK GDPR.

A Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The right to object to direct marketing must be made clearly and plainly to the individual.

An individual's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible.

25. COMPLAINTS

An individual has the right to make a complaint if they feel that their personal information has not been handled by the University in accordance with the Data Protection legislation. A complaint may be submitted in writing to the Data Protection & Information Compliance Manager. Alternatively, a complaint may be made to the Office of the Information Commissioner.

26. DPO & UNIVERSITY CONTACTS

Data Protection Officer

The DPO is responsible for overseeing this Data Protection Policy.

The University DPO is Eoin Coyle, who can be contacted at 028 71171 675525, e.coyle2@ulster.ac.uk / gdpr@ulster.ac.uk or at the Coleraine Campus, Room J308, Coleraine, BT52 1SA.

Please contact the DPO with any questions about the operation of this Data Protection Policy or if you have any concerns that this Data Protection Policy is not being or has not been followed.

Policy Coordinator

The DPO is supported by the Policy Co-ordinator. The Policy Co-ordinator is Jemma Bacon, Data Protection & Information Compliance Unit and can be contacted at 02870 124114 j.bacon@ulster.ac.uk / gdpr@ulster.ac.uk, Coleraine Campus, Room J306.

The DPO and Policy Co-ordinator are the first point of contact for queries and advice on responsibilities and compliance under this Policy.

Senior Leadership Team

In addition, the Vice-Chancellor, the Senior Leadership Team, Heads of School, Research Institute Directors and Heads of Professional Service Departments play a key role in assisting the DPO and for ensuring the University staff within their department, school, or office (as the case may be) comply with this Data Protection Policy and need to implement appropriate practices, controls and training to ensure such compliance.

Data Protection Nominees

A number of senior officers have been selected as “Data Protection Nominees” who have undertaken specialist data protection training. The Data Protection Nominees work with the DPO and Policy Coordinator to respond to requests and queries received from Data Subjects including Subject Access Requests and provide support in drafting Data Protection Impact Assessments. The Data Protection Nominees also assist with disseminating information in respect of the University’s data protection practices to ensure compliance and good practice across the University, in a coordinating role. Data Protection Nominees will liaise with the DPO and Policy Coordinator to identify Data Protection topics that may benefit of increased awareness and guidance. A list of Data Protection Nominees is available on Data Protection SharePoint site (to be updated)

Appendix 1

Glossary

Automated Decision-Making	when a decision is made which is based solely on Automated Processing (including profiling). The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.
Automated Processing	any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, such as to analyse or predict aspects concerning that individual's performance, personal preferences, interests, behaviour, location or movements.
Controller	means the person or organisation that determines when, why and how to process Personal Data. The University is a data Controller and is registered with the ICO (registration number Z6533200).
Criminal Offence Data	means Personal Data relating to criminal convictions and offences or related security measures which shall include allegations of offences by the Data Subject and proceedings or a committed or alleged offence by the Data Subject or disposal of the proceedings including sentencing.
Data Protection Legislation	shall mean: (i) the DPA 2018; (ii) the UK GDPR; (iii) the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426); (iv) any laws which implement or amend an such laws in the UK from time to time; (v) the guidance codes of practice issued by the Commissioner or other supervisory authority; and (vi) where applicable, other non-domestic legislation in force from time to time which may apply to the University's use of Personal Data.
Data Subject	means a living identified or identifiable individual about whom the University holds Personal Data. For the University, Data Subjects include current, past and present students and staff (including affiliated and visiting staff), and other third parties such as suppliers, contractors, consultants or referees.
DPA 2018	means the Data Protection Act 2018.
DPIA or Data Privacy Impact Assessment	means the tools and assessments used to identify and reduce risks of a data processing activity. A DPIA

	should be conducted for all major system or business change programs involving the processing of Personal Data.
DPO or Data Protection Officer	the data protection officer appointed by the University.
ICO	means the independent regulator and supervisory authority in the UK pursuant to section 114 DPA 2018.
Personal Data	means any information which identifies a Data Subject, or, information relating to a Data Subject that the University can identify (directly or indirectly) from that data alone or in combination with any other a Data Subject.
Personal Data Breach	any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that the University or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Processing Process or **Processes**	means any activity that involves the use of Personal Data. It includes, but is not limited to, any operation which is performed on the Personal Data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.
Related Policies	the University's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data as listed at appendix two.
Special Category Data	means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or data revealing physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.
UK GDPR	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.
University Staff	means all University employees including permanent and temporary employees, casual staff, postgraduate researchers, agency workers and contractors.

Appendix 2

Related Policies, Forms and Guidance

Ulster University Retention & Disposal Schedule
https://www.ulster.ac.uk/__data/assets/pdf_file/0009/286461/Records-Retention-and-Disposal-Schedule.pdf

Freedom of Information
https://www.ulster.ac.uk/about/governance/compliance/freedom-of-information
https://www.legislation.gov.uk/ukpga/2000/36/contents

Data Protection
https://www.ulster.ac.uk/about/governance/compliance/gdpr
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
https://ulster.sharepoint.com/sites/DataProtection

Equality Scheme:
https://www.ulster.ac.uk/peopleandculture/employee-benefits/equality-diversity/summary-of-the-equality-scheme

University Wide Policies and Procedures
https://www.ulster.ac.uk/about/governance/policies

Staff Discipline Procedures
https://www.ulster.ac.uk/peopleandculture/policies/disciplinary-procedures