ULSTER UNIVERSITY
GENERAL DATA PROTECTION REGULATION POLICY

1 INTRODUCTION and DEFINITIONS

The General Data Protection Regulation (**"GDPR"**) came into force across the European Union and together with the Data Protection Act 2018 **("DPA")**, replaced the UK Data Protection Act 1998. The purpose of the GDPR and DPA is to enhance and strengthen the protections afforded to individuals' rights and freedoms especially their right to privacy with respect to the processing of personal data. Due to the nature of business at Ulster University ("**University**") it is required to hold and process, both electronically and manually, large amounts of personal data. The GDPR and DPA provide a framework to ensure that personal information processed and stored by the University whether in hard copy or electronic format is handled properly both on and off campus.

1.1 Definitions and Meanings

1.1.1 " Controller"	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the Processing of personal data. The University is a data Controller.
1.1.2 "Data Subject"	means an identified or identifiable natural person about whom Personal Data is held. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, ID number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. 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.
1.1.3 "Personal Data"	means any information relating to a Data Subject. It includes, by way of example only, name, date of birth, images and photographs.
1.1.4 "Processing"	means any operation which is performed on Personal Data, whether or not by automated means, 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.
1.1.5 "Processor "	means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

1.1.6. "Special Categories of Personal Data"	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning physical or mental health or data concerning a person's sex life or sexual orientation.

1.2 APPLICATION

The GDPR works in two ways. Firstly, it sets out the main responsibilities for organisations in relation to the Processing of Personal Data whereby they must comply with the six principles contained within the GDPR. The second area covered by the GDPR provides a Data Subject with important rights, including the right to be informed, the rights of access, rectification, erasure, restriction of processing, data portability, objection and rights in relation to automated decision making and profiling (see section 12 below).

2 REGISTRATION

The University as a Controller must provide prescribed information to the Information Commissioner's Office **("ICO")** as well as pay a data protection fee annually. The ICO is the independent supervisory authority set up to promote and oversee compliance with data protection legislation in the UK. You can inspect the University's details on the ICO's data protection register at: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

The ICO has the right to carry out investigations in the form of a data protection audit on the University.

3 POLICY STATEMENT

The University is committed to protecting the rights of individuals in accordance with the provisions of the GDPR and DPA.

4 AIMS OF THE POLICY

The aims of this Policy are to set out the University's strategy for ensuring compliance with the GDPR and DPA, to ensure that all staff, students or third party Processors engaged by the University, are aware of their rights and responsibilities under the GDPR and DPA and to minimize the risk to the University of any potential breach of the GDPR or DPA. A breach of the GDPR or DPA could result in damaging valued relationships with stakeholders as well as causing reputational damage to the University and the individual.

This Policy relates to all Personal Data as defined by the GDPR held by the University and applies equally to information held in paper and electronic format stored in hard files, on PCs, laptops and other fixed or portable data storage devices. The Policy also applies to photographic material and CCTV footage.

5 THE DATA PROTECTION OFFICER AND OTHER STAFF CONTACTS

The University will ensure that it has in place at all times a designated Data Protection Officer.

The University Secretary, Mr Eamon Mullan, is the University's designated Data Protection Officer. The Data Protection Officer has the primary responsibility for coordinating Data Protection compliance across the University, including reporting, and is the ultimate arbitrator within the University in respect of Data Protection matters.

The Data Protection Officer is supported by the Policy Co-ordinator. The Data Protection Officer and Policy Co-ordinator are the first point of contact for queries and advice on responsibilities and compliance under the GDPR and DPA; for requests and objections by Data Subjects including subject access requests (see section 12); and for liaising with the ICO and other agencies where appropriate. Contact details for these officers are attached at Appendix 1.

In addition, the Vice-Chancellor, Deputy Vice-Chancellors, Chief Operating Officer, Deans, Provosts, Heads of School, Research Institute Directors and Directors/Heads of professional services departments play a key role in assisting the University's Data Protection Officer and are responsible for having in place appropriate procedures to ensure compliance with the GDPR and DPA within their areas of responsibility across the University. A list of these senior officers is attached at Appendix 2. These officers have nominated a suitable representative(s) **("Data Protection Nominee(s)")** who have undertaken specialist data protection training and work with the Data Protection Officer and Policy Co-ordinator to respond to requests and objections by Data Subjects including subject access requests (see section 12 below) and in relation to implementation and dissemination of good practice. Contact details for the Data Protection Nominees are also attached at Appendix 2.

6. GDPR PRINCIPLES

The University is committed to the six data protection principles contained within the GDPR. These principles represent best standards of practice with respect to the transmission, retention and disposal of Personal Data. All staff, students and others who process or use any Personal Data must comply with these principles. These state that Personal Data must:

i) be processed lawfully, fairly and in a transparent manner in relation to the Data Subject (**"lawfulness, fairness and transparency").** (Further details in relation to "lawfulness" and having a "lawful basis" for Processing is contained in section 7 below);

ii) be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes **("purpose limitation")**;

iii) be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed **("data minimisation")**;

iv) be accurate, kept up to date and if inaccurate erased or rectified **("accuracy")**;

v) be kept for no longer than is necessary for the purpose(s) for which the Personal Data is Processed **("storage limitation")**; and

vi) be Processed securely, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures **("integrity and confidentiality").**

The University, as Controller, is responsible for and must be able to demonstrate compliance with the six data protection principles.

7. LAWFUL BASIS FOR PROCESSING

For Processing of Personal Data to be lawful, all staff, students and others who process Personal Data must identify specific grounds for the Processing. This is called a "lawful basis" and there are six options Article 6 of the GDPR which depend on the purpose of the Processing and the relationship with the Data Subject. Article 6 of the GDPR is available online at: https://gdpr-info.eu/art-6-gdpr/

If Special Categories of Personal Data are being Processed, this is more sensitive and so requires more protection and so both (i) a "lawful basis" for general Processing (under Article 6 of the GDPR) is required, plus (ii) an additional condition for Processing under Article 9 GDPR. Article 9 GDPR is available online at : https://gdpr-info.eu/art-9-gdpr/

A "lawful basis" must be established before Processing begins and should be documented. If no "lawful basis" applies then the Processing will be unlawful and in breach of the GDPR principles.

The "lawful bases" for Processing as set out in Article 6 of the GDPR are as follows :

(i) **Consent:** the individual has given clear consent to process their Personal Data for a specific purpose.

(ii) **Contract:** the Processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

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

(iv) **Vital interests:** the Processing is necessary to protect someone's life.

(v) **Public task:** the Processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

(vi) **Legitimate interests:** the Processing is necessary for your 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. This cannot apply if you are a public authority Processing data to perform your official tasks.

At least one of these "lawful bases" must apply whenever Personal Data is being Processed.

8 RESPONSIBILITIES OF STAFF AND STUDENTS

Staff and students at the University are expected to read and understand this Policy and, where required, to seek further clarification from the office of the Data Protection Officer. Staff and students are required to abide by this Policy and related policies (see Appendix 3) as from time-to-time amended. Any alleged breaches of the GDPR or DPA by staff and/or students will be fully investigated and may result in disciplinary action and may, in some instances, be considered gross misconduct. **It is compulsory for all staff to complete the University's data protection training programme.**

All staff and students must apply the criteria listed below as appropriate and relevant at all times to the Processing of Personal Data in both electronic and hard copy format.

i) Ensure that data is kept securely in terms of physical security of offices and filing cabinets with the level of security appropriate to the level of confidentiality and sensitivity of the material.

ii) Ensure that robust procedures using appropriate technical or organisational measures are in place to prevent accidental loss, destruction or damage of Personal Data or unauthorised or unlawful Processing.

iii) Ensure that the use of, and access to, computers, laptops and other portable electronic data processing/storage devices is compliant with University guidance contained within the Code of Practice for Use of Ulster University Computer Networks, Equipment and Telephone Systems, available at: https://www.ulster.ac.uk/isd/it-policies

iv) Staff who have responsibility for supervising students involved in work which requires the Processing of Personal Data are required to ensure that the students are fully aware of the data protection principles and the requirements of this Policy, and the need to obtain the consent of any Data Subjects involved as appropriate.

v) Ensure that access to Personal Data is restricted only to authorised persons.

vi) Inform University security staff immediately of incidents where persons without proper authorisation are found in areas where Personal Data is held or processed.

vii) Ensure that Personal Data is retained only for the period of time for which it is required and for no longer than is necessary for the purpose for which the Personal Data is Processed. Further information on the length of time records should be kept can be found in the University's Retention and Disposal Schedule available at: https://www.ulster.ac.uk/__data/assets/pdf_file/0009/286461/Records-Retention-and-Disposal-Schedule.pdf

viii) Ensure that all Personal Data is obtained for specified, explicit and legitimate purposes and only processed for those purposes.

ix) Ensure that all Personal Data is processed lawfully, fairly and transparently with a "legal basis" for processing (see sections 6 and 7 above).

x) Ensure that all Personal Data collected or otherwise Processed is adequate, relevant and limited to what is necessary in relation to the purpose for which it is Processed.

xi) Avoid, in so far as possible, recording personal opinions not based on fact about a Data Subject. These comments will be disclosable.

xii) Ensure that Personal Data is processed securely and not disclosed either accidentally or deliberately either verbally or in writing to any unauthorised person or organisation.

xiii) Avoid giving Personal Data by telephone unless there is a very high degree of certainty that the caller is the person he/she claims to be, and is an appropriate person to receive the data in question.

xiv) Ensure that accurate, up-to-date personal details are provided to the University and notify the University immediately of any changes or errors. Inaccurate Personal Data must be erased or rectified immediately.

xv) There may be circumstances when it is appropriate for the University to share personal information with other organisations, for example if it relates to a criminal investigation. In any such circumstances further guidance should be sought from the Data Protection Officer.

9. PRIVACY NOTICES

The GDPR requires that the University must inform Data Subjects when, why and how their Personal Data is used by the University. Privacy notices should include the following information:

(i) Name and contact details of the University, its representative (as applicable) and Data Protection Officer;

(ii) Purpose of the Processing of Personal Data;

(iii) Lawful basis for Processing Personal Data (and the legitimate interests for Processing (if applicable) (see section 7 above);

(iv) The categories of Personal Data obtained (if the Personal Data is not obtained from the individual) ;

(v) Who the Data Subject's Personal Data is shared with, the recipients or categories of recipients of the Personal Data;

(vi) Details of international Personal Data transfers to any third countries or international organisations (if applicable);

(vii) How long the individual's Personal Data is held (retention periods);

(viii) Rights of the individual as a Data Subject;

(ix) Right to withdraw consent (if applicable);

(x) Right to lodge a complaint with the ICO;

(xi) The source of the Personal Data (if the Personal Data is not obtained from the individual);

(xii) The details of whether individuals are under a statutory or contractual obligation to provide the Personal Data (if applicable, and if the Personal Data is collected from the individual); and

(xiii) The details of the existence of automated decision-making, including profiling (if applicable).

In addition, section 12.1(i) below, provides further information relating to a Data Subject's right to be informed. A number of the University's privacy notices meanwhile are available online at: https://www.ulster.ac.uk/about/governance/gdpr.

10. DATA PROTECTION IMPACT ASSESSMENTS

A data protection impact assessment **("DPIA")** is a process to help identify and minimise the data protection risks of a project. A DPIA must be done for Processing that is **likely to result in a high risk** to individuals. This includes some specified types of Processing. It is also good practice to do a DPIA for any other major project which requires the processing of Personal Data.

Please email gdpr@ulster.ac.uk for further guidance as required.

11. PERSONAL DATA BREACHES

11.1 Definition of a Personal Data Breach of the GDPR

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed **("Personal Data Breach")**.

There is an obligation on the University to report certain types of Personal Data Breach to the ICO without undue delay and, where feasible, not later than ***72 hours*** after having become aware of it. If the breach is likely to result in a high risk to the individuals' rights and freedoms, the University must also inform those individuals without undue delay. The University must keep a record of any Personal Data Breaches, their effects and the remedial action taken.

11.2 Fines

In the event of an infringement of the GDPR, the ICO has the power to impose fines
(in more serious cases) of up to 20 million euros or in the case of an undertaking up to 4% of annual turnover whichever is higher.

11.3 What Events/Incidents should be reported to the Data Protection Officer?

Any 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
- Unauthorised disclosure of personal information
- Loss of personal files
- Non arrival of sensitive information
- Maintenance of unsecured databases

The above list is not exhaustive

11.4 When should a Personal Data Breach be reported to the Data Protection Officer ?

Immediately in all cases once the Personal Data Breach has been discovered.

11.5 **How should the Personal Data Breach be reported?**

By completing the Personal Data Breach Report Form attached as Appendix 5 to this Policy.

The completed Report Form should be forwarded immediately to the University Secretary and Data Protection Officer, Mr Eamon Mullan, c/o Ulster University, Room J312 Coleraine, BT52 1SA or via email at: e.mullan@ulster.ac.uk. Mr Mullan's office will contact you in confidence on receipt of the report form. If you require any advice please contact Mr Mullan on telephone no. 028 701 24533. In the case of complainants, complaints may also be made directly to the Information Commissioner's Office (ICO). Details of how to complain to the ICO are detailed in this Policy under section 16 below.

12. RIGHTS OF DATA SUBJECTS

12.1 Under the GDPR, an individual 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 GDPR.

Data Subjects must be provided with information including: the purpose(s) for processing their Personal Data, the retention periods and who it will be shared with. This is called 'privacy information' and must be provided to individuals at the time Personal Data is collected from them. The information provided must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language. Privacy information must be regularly reviewed, and where necessary updated. Any new uses of an individual's Personal Data must be brought to their attention before Processing commences.

If Personal Data is obtained from other sources, individuals must be provided with privacy information within a reasonable period of obtaining the data and no later than one month.

There are a few circumstances when privacy information does not need to be provided, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

Further information in relation to Privacy Notices is contained in section 9 above. In addition, see Articles 13 and 14 of the GDPR available online at: https://gdpr-info.eu/art-13-gdpr/ and https://gdpr-info.eu/art-14-gdpr/

(ii) **The right of access to your Personal Data (Subject Access Request("SAR"))**

A Data Subject has the right to request access to their Personal Data held by the University. A SAR 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.

If a SAR is received by any member of staff it should be forwarded immediately to the Data Protection Officer via email to gdpr@ulster.ac.uk. Staff guidance on SARs is available at: https://www.ulster.ac.uk/about/governance/compliance/gdpr/data-subject-rights/right-of-access

Any person who wishes to exercise this right meanwhile is required to make their request either verbally on telephone no. 028 701 24533 or by email to: gdpr@ulster.ac.uk

See Article 15, GDPR available online at: https://gdpr-info.eu/art-15-gdpr/

(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 (See Article 16, GDPR available online at: https://gdpr-info.eu/art-16-gdpr/)

Under Article 18 of the GDPR, a Data Subject has the right to request restriction of the Processing of their Personal Data where they contest its accuracy and the University is checking it. See section 12.1 (v) below for further details in this regard.

(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. See Article 17 of the GDPR for further information, available online at: https://gdpr-info.eu/art-17-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 the GDPR, available at: https://gdpr-info.eu/art-18-gdpr/

This right involves limiting the way in which the University can use an individual's Personal Data. It is an alternative to requesting the erasure of Personal Data.

(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 the GDPR, available at: https://gdpr-info.eu/art-20-gdpr/

This right allows Data Subjects to obtain and reuse their Personal Data for their own purposes across different services. It allows them to move, copy or transfer Personal Data easily from one IT environment to another in a safe and secure way without affecting its usability. This right only applies to Personal Data that a Data Subject has provided to the University.

(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 the GDPR, available at https://gdpr-info.eu/art-21-gdpr/

It includes a right to object to Processing (including profiling) of their data that proceeds under particular legal bases; to direct marketing; and to processing of their data for research purposes where that research is not necessary in the public interest.

(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 the GDPR, available at: https://gdpr-info.eu/art-22-gdpr/

12.2 Exercising Data Subject Rights:

Any person who wishes to exercise any of those rights detailed at points (i) to (viii) above, is required to make their request either verbally on telephone no. 028 701 24533 or by email to gdpr@ulster.ac.uk.

If a request to exercise any of those rights detailed at points (i) to (viii) above meanwhile, is received by any member of staff it should be forwarded immediately to the Data Protection Officer by email to gdpr@ulster.ac.uk.

The University does not normally charge a fee to process such requests. However, where the request is manifestly unfounded or excessive, the University may charge a reasonable fee for the administrative costs of complying with the request, or refuse to comply with the request (taking into account whether the request is repetitive in nature).

The University undertakes to consider and if appropriate act upon a request without undue delay. In compliance with the law, 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.

In the event that the University refuses to comply with a request, it will inform the individual without undue delay and within one month of receipt of the request. In such circumstance, the University shall explain its reasons for not taking the action, and inform the individual of their right to make a complaint to the ICO and of their ability to seek to enforce this right through a judicial remedy.

Where the University has doubts concerning the identity of the individual making the request, the provision of additional information necessary to confirm the identity of the data subject (for example, photographic proof of identity) may be requested prior to acting upon a request. The University shall let the Data Subject know without undue delay and within one month if it needs such additional information. The University does not need to act upon a request until it has received the additional information.

Rights in relation to automated decision making and profiling:

The University undertakes to consider an objection without undue delay. In compliance with the law, the University will confirm the action it has taken within one month of receipt of an objection.

In the event that the University refuses to comply with an objection, it will similarly inform the individual without undue delay and within one month of receipt of the objection. In such circumstances, the University shall explain its reasons for not taking the action and inform the individual of their right to challenge or appeal such decision, and the grounds on which they can appeal.

13. ACCOUNTABILITY

The University, as Controller, shall be responsible for, and be able to demonstrate compliance with the Data Protection principles and the rights of individuals detailed above.

The GDPR introduces a range of accountability requirements which encourages the University to take a proactive and documented approach to compliance. These accountability requirements include:

13.1 Implementing policies, procedures, processes and training to promote "data protection by design and by default".

13.2 Having appropriate contracts in place when outsourcing functions that involve the Processing of Personal Data (see section 14 below).

13.3 Implementing appropriate security measures.

13.4 Maintaining records of the Data Processing that is carried out across the University.

13.5 Documenting and reporting Personal Data breaches (see section 11 above).

13.6 The obligation to carry out a Data Protection Impact Assessment before carrying out types of Processing "likely to result in a high risk "to individuals" (see section 10 above).

13.7 Appointing a Data Protection Officer (see section 5 above).

13.8 Adhering to relevant codes of conduct and signing up to certification schemes.

14. USE OF PERSONAL DATA BY PROCESSORS AND OTHER DATA SHARING ARRANGEMENTS

Where a Processor including for example, consultants or contractors are engaged by the University on work that requires the Processing of Personal Data, the University remains the Controller of that Personal Data and these organisations will be required to provide sufficient guarantees to demonstrate that they have arrangements in place to comply with the requirements of the GDPR and DPA, this Policy and that the rights of Data Subjects are protected. Whenever the University uses a Processor it must have a written contract in place. In line with this Policy, a Third Party Processing Agreement (**"Agreement**") must be used when engaging such Processors (or alternatively, duplicate provisions can be included within the corresponding "main

contract" as appropriate). A template Agreement and guidance in relation to its use is available upon request from the Office of the University Secretary by emailing gdpr@ulster.ac.uk

It should be noted that Processors must only act on the documented instructions of the University as the Controller. The Processor will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

It should be noted that Personal Data Processing arrangements (as outlined above) form only one category of data sharing. There are 3 broad categories, including the sharing of Personal Data with another Data Controller to be used for joint purposes and also the passing of Personal Data to a Data Controller for it to use for its own purposes. Further guidance and template documents as required for use in relation to such data sharing arrangements are available upon request from the Office of the University Secretary by emailing gdpr@ulster.ac.uk.

15. INTERNATIONAL TRANSFERS

There are restrictions imposed on the University by the GDPR when transferring Personal Data outside the European Economic Area **("EEA")**. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined. Personal Data can only be transferred outside of the EEA in compliance with the conditions for transfer set out in Chapter V of the GDPR - https://gdpr-info.eu/chapter-5/

Transferring Personal Data outside of the EEA is a complex process which requires a strict procedure to be followed in order for such transfer to be lawful. For further guidance in this regard, please contact the Office of the University Secretary by emailing gdpr@ulster.ac.uk.

16. COMPLAINTS

Under Article 77 of the GDPR, available at: http://www.privacy-regulation.eu/en/article-77-right-to-lodge-a-complaint-with-a-supervisory-authority-GDPR.htm, 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 GDPR. A complaint may be submitted in writing to the Data Protection Officer, Mr Eamon Mullan, c/o Ulster University, Room J312, Coleraine, BT52 1SA or by email at: gdpr@ulster.ac.uk. Alternatively, a complaint may be made to the Office of the Information Commissioner. Full particulars including contact details and the information leaflet 'When and How to Complain' may be found at: https://icosearch.ico.org.uk/s/search.html?query=HOW+TO+COMPLAIN&collection=ico-meta&profile=_default

17. POLICY IMPLEMENTATION

The University will ensure that this Policy and the appropriate procedures are implemented and disseminated and are kept under regular evaluation and review.

18. FURTHER INFORMATION

Some sources of further information are set out in Appendix 4.

APPENDIX 1

OFFICE OF THE UNIVERSITY SECRETARY
CONTACTS

Data Protection Officer	Mrs Clare Jamison Telephone No: +44 (028) 7012 3502 e-mail: c.jamison@ulster.ac.uk
Legal Services Manager	Mrs Alison Kerr Telephone No: +44 (028) 7012 3329 e-mail: a.kerr@ulster.ac.uk
Policy Co-ordinator	Ms Elinor Byrden Telephone No: +44 (028) 7012 3354 e-mail: e.byrden@ulster.ac.uk

APPENDIX 2

SENIOR OFFICERS AND DATA PROTECTION NOMINEES CONTACTS

Department		**GDPR Trained Nominees**	**Contact Details for Nominees**
Student Administration & Registry	Ruth Wasson	Pamela McCafferty	Tel : 028 9036 8172 Email: ph.mccafferty@ulster.ac.uk
People & Culture	Damian McAlister	Christine Hayes	Tel: 028 7012 3260 Email: c.hayes@ulster.ac.uk
Development & Alumni Relations	Eddie Friel	Alison Snookes	Tel: 028 7012 4460 Email: a.snookes@ulster.ac.uk
Strategy, Planning & Performance	Vice-Chancellors Office	Catherine McCollum	Tel: 028 7012 4559 Email: c.mcclements@ulster.ac.uk
Corporate Events	Vice-Chancellor's Office	Alison Milne	Tel: 028 9036 6948 Email: ae.milne@ulster.ac.uk
Life & Health Sciences	Carol Curran	Brian McAuley	Tel: 028 7012 3064 Email: b.mcauley@ulster.ac.uk
Ulster Business School	Mark Durkin	Tom O'Neill	Tel: 028 9036 8126 Email: t.oneill@ulster.ac.uk
Computing, Engineering & the Built Environment	Liam Maguire	Philip Doherty	Tel: 028 9539 7421 Email: pj.doherty@ulster.ac.uk
Arts, Humanities & Social Sciences	Paul Seawright	Catherine Brown	Tel: 028 9036 8009 Email: cf.brown@ulster.ac.uk
Research & Impact	Cathy Gormley-Heenan	Nick Curry	Tel: 028 9036 6629 Email: n.curry@ulster.ac.uk
Finance	Peter Hope	Hilary Hogg	Tel: 028 7012 3288 Email: h.hogg@ulster.ac.uk
		Wayne Robinson	Tel: 028 9036 6150 Email: w.robinson@ulster.ac.uk
Digital & Information Services	Richard Millar	Stephen McAlister	Tel: 028 7012 3324 Email: s.mcalister@ulster.ac.uk
		Janet Peden	Tel: 028 7012 4743 Email: je.peden@ulster.ac.uk
		Elizabeth Young	Tel: 028 9036 8181 Email: es.young@ulster.ac.uk
Chief Operation Officer	Niamh Lamond	Lauren Stuart	Tel: 028 9536 7033 Email: l.stuart@ulster.ac.uk

Provosts	Vice-Chancellor's Office	Sarah Gallagher	Tel: 028 7167 5083 Email: sarah.gallagher@ulster.ac.uk
Global Engagement	Cathy Gormley-Heenan	Claire Johnston	Tel: 028 9536 7042 Email: c.johnston1@ulster.ac.uk
Estates	Michael Fitzpatrick	Jean Sharpe	Tel: 028 7012 3017 Email: j.sharpe@ulster.ac.uk
Student Support	Amanda Castray	Claire Drummond	Tel: 028 9036 6602 Email: c.drummond@ulster.ac.uk
Marketing & Communications	Joanne McGowan	Catherine McKeown	Tel: 028 9036 6086 Email: c.mckeown@ulster.ac.uk

APPENDIX 3

OTHER RELATED UNIVERSITY POLICIES, FORMS AND GUIDANCE

Code of Practice for Use of Ulster University Computer Networks, Equipment and Telephone Systems, available at:
https://www.ulster.ac.uk/isd/it-policies

Ulster University Retention and Disposal Scheme:
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

Guide to the General Data Protection Regulation (GDPR)
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Student Handbook:
https://www.ulster.ac.uk/connect/guide?s=student+handbook

Policy for the Protection of Children and Vulnerable Adults:
http://www.ulster.ac.uk/guide/useful-info/policies/protection-of-children-and-vulnerable-adults/

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

Disability Disclosure Guidelines:
https://www.ulster.ac.uk/__data/assets/pdf_file/0008/119807/Disability-Disclosure-Guidelines-for-Academic-and-Faculty-Support-Staff.pdf
https://www.ulster.ac.uk/studentsupport/services/disability/accessability/new-students

Special Educational Needs and Disability (NI) Order 2005 - Guidance
https://www.ulster.ac.uk/__data/assets/pdf_file/0007/119815/Revised-SENDO-Staff-Guidance-Booklet-2016.pdf

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

APPENDIX 4

FURTHER RELEVANT INFORMATION IS AVAILABLE AT:

The General Data Protection Regulation, in full at:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

The Data Protection Act 2018
https://www.gov.uk/government/collections/data-protection-act-2018

Law Enforcement Directive (Directive (EU) 2016/680), in full at:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873

Privacy and Electronic Communications Regulations in full at:
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058

Higher Education Statistics Agency:
https://www.hesa.ac.uk/

Information Commissioner's website:
https://ico.org.uk/

Joint Information Systems Committee (JISC) Legal Information Service:
https://www.jisc.ac.uk/guides/data-protection

APPENDIX 5

ULSTER UNIVERSITY
GENERAL DATA PROTECTION REGULATION
PERSONAL DATA BREACH REPORT FORM

NAME……

ADDRESS……

TELEPHONE …… **E-mail address**…….

A) Please tick as appropriate:

I am a registered student ☐ my registration number is:…….

I am a member of staff ☐

in the Faculty/School or Department of……..

I am not a staff member or student ☐

My association with the University consists of:……

……

B) What incident do you want to report or (as applicable) complain about? (Name of Department/Faculty/School)

……

C) Details of incident/complaint (as applicable):

.....……..……

……...……

……...……

……...

……...……

……

……

……...……...

D) When did you first become aware of the problem?

……

E) Have you reported details of the incident/complaint (as applicable) to anyone else in the University?

……

……...……

F) Supporting Documents - Please attach any supporting documentation.

SIGNED:……

DATE:……

When completed this form should be returned to Mrs Clare Jamison, University Secretary and Data Protection Officer , University of Ulster, Cromore Road, Coleraine BT52 1SA. The form can also be emailed to gdpr@ulster.ac.uk