ULSTER UNIVERSITY
GENERAL DATA PROTECTION REGULATION POLICY

1 INTRODUCTION and DEFINITIONS

The General Data Protection Regulation (**"GDPR"**) applies in the UK and the rest of the EU from 25 May 2018, replacing the Data Protection Act 1998. The purpose of the GDPR 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 provides 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 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 9 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

Ulster University is committed to protecting the rights of individuals in accordance with the provisions of the GDPR.

4 AIMS OF THE POLICY

The aims of this Policy are to set out the University's strategy for ensuring compliance with the GDPR, 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 to minimize the risk to the University of any potential breach of the GDPR. A breach of the GDPR 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 GDPR PRINCIPLES [1]

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 fairly, lawfully and transparently in relation to the individual (as part of this, the University must have a "legal basis" for processing an individual's Personal Data. For example, the individual has consented to the Processing, or the Processing is necessary to operate a contract with them, to fulfil a legal obligation, for a vital interest; to perform a public task or for a legitimate interest. See Article 6 of the GDPR. In addition, Special Categories of Personal Data are more sensitive and so need more

[1] *Summarised from the Data Protection Act 1998 © Crown Copyright 1998*

protection and so both a lawful basis and a separate condition for Processing under Article 9 of the GDPR must be identified. In addition, in relation to children the GDPR introduces special protection for children's Personal Data.) (**"lawfulness,fairness and transparency")**;

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")**;

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")**

6 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. These officers are the first point of contact for queries and advice on responsibilities and compliance under the GDPR; for requests and objections by Data Subjects including subject access requests (see section 9); and for liaising with the ICO and other agencies where appropriate. Contact details for these officers are attached at Appendix 1.

7 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 2) as from time-to-time amended. Any alleged breaches of the GDPR 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/about/governance/compliance/data-protection

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 fairly, lawfully and transparently with a "legal basis" for processing (see Section 10).

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 accidently 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.

The Vice-Chancellor, Pro-Vice-Chancellors, Chief Operating Officer, Deans, Provosts, Heads of School, Research Institute Directors and Directors/Heads of professional services departments are responsible for having in place appropriate procedures to ensure compliance with the GDPR within their areas of responsibility. These officers will also be responsible for nominating a suitable representative(s) who will undertake specialist data protection training and will work with the Data Protection Officer to respond to requests and objections by Data

Subjects including subject access requests (see Section 9) and implementation and dissemination of good practice.

8. BREACH OF THE GDPR

8.1 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. 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.

8.2 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.

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

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

8.4 When Should the Event/Incident be reported?

Immediately the data loss has been discovered.

8.5 How should the Event/Incident be reported?

By completing the Breach of Data Security Report Form attached as Appendix 4 to this Policy. The Report Form is also available online at:
https://www.ulster.ac.uk/about/governance/compliance/data-protection
The completed Report Form should be forwarded to the University Secretary and Data Protection Officer,Mr Eamon Mullan, c/o University of Ulster, Room J312 Coleraine, BT52 1SA. A copy of the Report Form can be emailed to Mr Mullan at: e.mullan@ulster.ac.uk. Mr Mullan will contact you in confidence on receipt of the Report Form. If you require any advice please contact Mr Mullan on telephone no. 028 7012 4533. 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 **13. COMPLAINTS.**

9 RIGHTS OF DATA SUBJECTS

Under the GDPR, an individual has the following rights (all of which rights are qualified in different ways) :

9.1 The right to be informed:

A Data Subject has the right to be informed of how their Personal Data is being used by the University. [In this regard, please see the University's privacy notice online at : https://www.ulster.ac.uk/about/governance/gdpr

9.2 **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.

Any person who wishes to exercise this right is required to complete a subject access form available upon written request to the Data Protection Officer, also available at: https://www.ulster.ac.uk/about/governance/compliance/data-protection

The University does not normally charge a fee to process subject access requests. However, where the request is manifestly unfounded or excessive, particularly if it is repetitive, the University may charge a reasonable fee or refuse to act on the request. The University may also charge a reasonable fee to comply with requests for further copies of the same information.

If a subject access request is received by any other member of staff it should be forwarded immediately to the Data Protection Officer.

The University undertakes to comply with requests for access to personal information without 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.

Where the University has reasonable 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 issue of Personal Data.

9.3 **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.

Any person who wishes to exercise this right is required to make their request either verbally or in writing to the Data Protection Officer. If in writing please complete a rectification request form available upon written request to the Data Protection Officer, also available at:
https://www.ulster.ac.uk/about/governance/compliance/data-protection
If a rectification request is received by any other member of staff it should be forwarded immediately to the Data Protection Officer.

The University does not normally charge a fee to process a rectification request. 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).

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 9.5 below for further details in this regard.

The University undertakes to consider and if appropriate act upon a request for rectification 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 without undue delay and within 1 month of the receipt of the request, together with the reasons for the delay.

In the event that the University is satisfied that the Personal Data is accurate, it will let the individual know and shall tell them that it will not be amending the Personal Data. In such circumstance, the University shall explain its decision and inform the individual of their right to make a complaint to the ICO and of their ability to seek to enforce their rights 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 rectification request until it has received the additional information.

9.4 **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) available online at:
http://www.privacy-regulation.eu/en/article-17-right-to-erasure-'right-to-be-forgotten'-GDPR.htm

Any person who wishes to exercise this right is required to make their request either verbally or in writing to the Data Protection Officer. If in writing please complete a request for erasure form available upon written request to the Data Protection Officer, also available at:
https://www.ulster.ac.uk/about/governance/compliance/data-protection

If an erasure request is received by any other member of staff it should be forwarded immediately to the Data Protection Officer.

The University does not normally charge a fee to process an erasure request. 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 for erasure 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 without undue delay and 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 for erasure, 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 an erasure request until it has received the additional information.

9.5 **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: http://www.privacy-regulation.eu/en/article-18-right-to-restriction-of-processing-GDPR.htm
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.

Any person who wishes to exercise this right is required to make their request either verbally or in writing to the Data Protection Officer. If in writing please complete a request to restrict processing form available upon written request to the Data Protection Officer, also available at:
https://www.ulster.ac.uk/about/governance/compliance/data-protection

If a request to restrict processing is received by any other member of staff it should be forwarded immediately to the Data Protection Officer.

The University does not normally charge a fee to process a request to restrict processing of Personal Data. 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 to restrict processing 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 for restriction, 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 to restrict processing until it has received the additional information.

9.6 **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: http://www.privacy-regulation.eu/en/article-20-right-to-data-portability-GDPR.htm

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.

Any person who wishes to exercise this right is required to make their request either verbally or in writing to the Data Protection Officer. If in writing please complete a request for data portability form available upon written request to the Data Protection Officer, also available at:
https://www.ulster.ac.uk/about/governance/compliance/data-protection

If a request for data portability is received by any other member of staff it should be forwarded immediately to the Data Protection Officer.

The University does not normally charge a fee to process a request for data portability of Personal Data. 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 for data portability 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 for data portability, 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 as soon as possible if it needs such additional information. The University does not need to act upon a request for data portability until it has received the additional information.

9.7 **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 http://www.privacy-regulation.eu/en/article-21-right-to-object-GDPR.htm

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.

Any person who wishes to exercise this right is required to make their objection either verbally or in writing to the Data Protection Officer. If in writing please complete an objection form available upon written request to the Data Protection Officer, also available at:
https://www.ulster.ac.uk/about/governance/compliance/data-protection

If an objection is received by any other member of staff it should be forwarded immediately to the Data Protection Officer.

The University does not normally charge a fee to comply with an objection to Processing Personal Data. 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 objection (taking into account whether the request is repetitive in nature).

The University undertakes to consider and if appropriate act upon an objection without undue delay. In compliance with the law, this will be at the latest within one month of receipt of an objection. 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 objection, together with the reasons for the delay.

In the event that the University refuses to comply with an objection, it will inform the individual without undue delay and within one month of receipt of the objection. 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 objection, 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 an objection. The University shall let the Data Subject know as soon as possible if it needs such additional information. The University does not need to act upon an objection until it has received the additional information.

9.8 **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: http://www.privacy-regulation.eu/en/article-22-automated-individual-decision-making-including-profiling-GDPR.htm

Any person who wishes to exercise this right is required to make their objection either verbally or in writing to the Data Protection Officer. If in writing please complete an automated decision making and profiling form available upon written request to the Data Protection Officer, also available at: https://www.ulster.ac.uk/about/governance/compliance/data-protection

If an automated decision making and profiling objection is received by any other member of staff it should be forwarded immediately to the Data Protection Officer. ***[Note – Additional provisions to be included here once further guidance is issued by the ICO on this point]***

10. 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:

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

10.2 Having appropriate contracts in place when outsourcing functions that involve the Processing of Personal Data (see section 11 below).

10.3 Implementing appropriate security measures.

10,3 Maintaining records of the Data Processing that is carried out across the University.

10.4 Documenting and reporting Personal Data breaches.

10.5 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".

10.6 Appointing a Data Protection Officer.

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

11 USE OF PERSONAL DATA BY PROCESSORS

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, 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 the University's Data Protection Policy the Third Party Processing Agreement (the Agreement) must be used when engaging such Processors. The Agreement is available at:
https://www.ulster.ac.uk/__data/assets/pdf_file/0006/119931/third_party_processing_agreement.pdf

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.

12. INTERNATIONAL TRANSFERS

There are restrictions imposed on the University by the GDPR when transferring Personal Data outside the European Union. 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 EU in compliance with the conditions for transfer set out in Chapter V of the GDPR - https://gdpr-info.eu/chapter-5/

13. 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 University of Ulster, Room J312, Coleraine, BT52 1SA or by email at: e.mullan@ulster.ac.uk. Alternatively, a complaint may be made to the Office of the Information Commissioner. Full particulars of the GDPR 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

14 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.

15 FURTHER INFORMATION

Some sources of further information are set out in Appendix 3.

APPENDIX 1

CONTACTS
2017/18

Data Protection Officer	Mr Eamon Mullan Telephone No: (028) 7012 4403 e-mail: e.mullan@ulster.ac.uk
Policy Co-ordinator	Ms Elinor Byrden Telephone No: (028) 7012 3354 e-mail: e.byrden@ulster.ac.uk

APPENDIX 2

OTHER RELATED UNIVERSITY POLICIES, FORMS and GUIDANCE 2018

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/about/governance/compliance/data-protection

Subject Access Request Form:
https://www.ulster.ac.uk/about/governance/compliance/data-protection

Freedom of Information:
https://www.ulster.ac.uk/about/governance/compliance/freedom-of-information

Student Handbook:
http://www.ulster.ac.uk/guide/

Child Protection Policy:
http://www.ulster.ac.uk/guide/useful-info/policies/protection-of-children-and-vulnerable-adults/

Equality Scheme:
http://www.equality.ulster.ac.uk/pdf/uuequalityscheme.pdf

Disability Disclosure Guidelines:
http://www.equality.ulster.ac.uk/2412-disclosure_guidelines.pdf

Special Educational Needs and Disability (NI) Order 2005 - Guidance
http://www.equality.ulster.ac.uk/1587-sendo_booklet.pdf

Note : Policies to be updated as required

APPENDIX 3

FURTHER RELEVANT INFORMATION IS AVAILABLE AT:

The General Data Protection Regulation, in full at :
https://gdpr-info.eu/

Law Enforcement Directive (Directive (EU) 2016/680), in full at:

The Data Protection Act 2018 (subject to Royal Assent) to the extent that it relates to processing of personal data and privacy:

Privacy and Electronic Communications Regulations in full at:
http://www.legislation.gov.uk/uksi/2003/2426/contents/made

Higher Education Statistics Agency:
http://www.hesa.ac.uk/dataprot/

Information Commissioner's website:
http://www.ico.gov.uk/

Joint Information Systems Committee (JISC) Legal Information Service:
http://www.jisclegal.ac.uk/dataprotection/dataprotection.htm]

Joint Information Systems Committee (JISC) Data Protection Code of Practice for the HE & FE Sectors:
http://www.jisc.ac.uk/publications/publications/pub_dpacop_0101.aspx]

APPENDIX 4

ULSTER UNIVERSITY
GENERAL DATA PROTECTION REGULATIONS
(Reg (EU) 2016/679)

BREACH OF DATA SECURITY – 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 do you want to complain about? (Name of Department/Faculty/School)

……...

C) Details of your complaint: ....……..

……...

……...

……

……...

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

……...

E) Have you reported your complaint to anyone else in the University? …..……..

……...

F) Supporting Documents - Please attach any supporting documentation

SIGNED: ……

DATE: ……

When completed this form should be returned to Mr Eamon Mullan, University Secretary and Data Protection Officer , University of Ulster, Room J313, Coleraine, BT52 1SA. The form can also be emailed to Mr Mullan at: e.mullan@ulster.ac.uk.