General Data Protection Regulation (GDPR) Policy

Effective date of the Policy:	March 2019
Previous Review of the Policy:	May 2018
Review Due on the Policy:	June 2020
Responsible SMT Member:	CEO
Policy Authorised By:	Board of Trustees
Signed:	Kevin McStravock, Chair of Board of Trustees
Date	25th February 2019

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 Students' Union ("UUSU") it is required to hold and process personal data, both electronically and manually. The GDPR provides a framework to ensure that personal information processed and stored by UUSU 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. UUSU 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, by reference to an identifier, such as a name, ID number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. For UUSU, Data Subjects include current, past and present students and staff, and other third parties such as suppliers, contractors, and consultants.

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 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 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

UUSU 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 UUSU'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 UUSU.

3. Policy Statement

UUSU 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 UUSU'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 minimise the risk to UUSU 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 UUSU and the individual.

This Policy relates to all Personal Data as defined by the GDPR held by UUSU 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 video footage.

5. GDPR Principles[1]

UUSU 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, UUSU 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 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

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

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

UUSU will ensure that it always has in place a designated Data Protection Officer.

The company CEO, Mr David Longstaff is UUSUs current designated Data Protection Officer. The Data Protection Officer has the primary responsibility for coordinating Data Protection compliance across UUSU, including reporting, and is the ultimate arbitrator within UUSU (in conjunction with the Board of Trustees) in respect of Data Protection matters. UUSU will also coordinate and work closely with Ulster University's Data Protection Officer, in the form of Mr Eamon Mullen, the Company Secretary.

The Data Protection Officer is 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. Full contact details are attached at Appendix 1.

7. Responsibilities of Staff and Students

Staff and students connected to UUSU 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 all associated policies 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. UUSU will share details of the University's data protection training programme for completion by staff.

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 UUSU guidance and follows Ulster University protocol contained within the relevant 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 senior management of UUSU 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 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 this document in appendix 2.

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 UUSU and notify your line manager (who will liaise with the Data Protection Officer) 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 UUSU 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.

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 UUSU 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, UUSU must also inform those individuals without undue delay. UUSU 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

NB: The above list is not exhaustive

8.4 When Should the Event/Incident be reported?
Immediately when 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 3 to this Policy. The completed Report Form should be forwarded to David Longstaff, CEO and Data Protection Officer, c/o UUSU, University of Ulster, Room 11H03, Jordanstown Campus, Shore Road, Newtownabbey BT37 0QB. A copy of the Report Form can be emailed to Mr Longstaff at: d.longstaff@ulster.ac.uk. Mr Longstaff will contact you in confidence on receipt of the Report Form. If you require any advice, please contact Mr Longstaff on telephone no. 028 90366053. 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 13.

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 UUSU. [In this regard, please see UUSUs privacy notice which can be viewed online.]

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 UUSU. Any person who wishes to exercise this right is required to complete a subject access form available online or upon written request to the Data Protection Officer.

UUSU 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, UUSU may seek advice from the ICO on charging a reasonable fee or refusing to act on the request. UUSU 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.

UUSU 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, considering the complexity and number of the requests. UUSU 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 UUSU 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 UUSU 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 make this written request to the Data Protection Officer. If a rectification request is received by any other member of staff it should be forwarded immediately to the Data Protection Officer.

UUSU does not normally charge a fee to process a rectification request. However, where the request is manifestly unfounded or excessive, particularly if it is repetitive, UUSU may seek advice from the

ICO on charging a reasonable fee or refusing to act on the request (considering 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 UUSU is checking it. See section 9.5 below for further details in this regard. UUSU 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, considering the complexity and number of the requests. UUSU 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.

If UUSU 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, UUSU 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 UUSU 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. UUSU shall let the Data Subject know without undue delay and within one month if it needs such additional information. UUSU 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 UUSU erased. This right is not absolute and only applies in certain circumstance. 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 make a written request to the Data Protection Officer. If an erasure request is received by any other member of staff it should be forwarded immediately to the Data Protection Officer.

UUSU does not normally charge a fee to process an erasure request. However, where the request is manifestly unfounded or excessive, particularly if it is repetitive, UUSU may seek advice from the ICO on charging a reasonable fee or refusing to act on the request (considering whether the request is repetitive in nature).

UUSU 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, considering the complexity and number of the requests. UUSU 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.

If UUSU 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, UUSU 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 UUSU 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. UUSU shall let the Data Subject know without undue delay and within one month if it needs such additional information. UUSU 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-torestriction-of-processing-GDPR.htm. This right involves limiting the way in which UUSU 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 make a written request to the Data Protection Officer. If a request to restrict processing is received by any other member of staff it should be forwarded immediately to the Data Protection Officer.

UUSU 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, particularly if it is repetitive, UUSU may seek advice from the ICO on charging a reasonable fee or refusing to act on the request (considering whether the request is repetitive in nature).

UUSU 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, considering the complexity and number of the requests. UUSU 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.

If UUSU 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, UUSU 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 UUSU 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. UUSU shall let the Data Subject know without undue delay and within one month if it needs such additional information. UUSU 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 UUSU. 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 a request for data portability is received by any other member of staff it should be forwarded immediately to the Data Protection Officer.

UUSU 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, particularly if it is repetitive, UUSU may seek advice from the ICO on charging a reasonable fee or refusing to act on the request (considering whether the request is repetitive in nature).

UUSU 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, considering the

complexity and number of the requests. UUSU 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.

If UUSU 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, UUSU 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 UUSU 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. UUSU shall let the Data Subject know as soon as possible if it needs such additional information. UUSU 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-toobject-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 an objection is received by any other member of staff it should be forwarded immediately to the Data Protection Officer.

UUSU does not normally charge a fee to comply with an objection to Processing Personal Data. However, where the request is manifestly unfounded or excessive, particularly if it is repetitive, UUSU may seek advice from the ICO on charging a reasonable fee or refusing to act on the request (considering whether the request is repetitive in nature).

UUSU 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, considering the complexity and number of the requests. UUSU 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.

If UUSU 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, UUSU 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 UUSU 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. UUSU shall let the Data Subject know as soon as possible if it needs such additional information. UUSU 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[2]

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

[2] Additional provisions will be included here once further guidance is issued by the ICO on this point

Article 22 of the GDPR, available at: http://www.privacy-regulation.eu/en/article-22-automatedindividual-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 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.

10. Accountability

UUSU, 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 UUSU to take a proactive and documented approach to compliance. These accountability requirements include: Implementing policies, procedures and processes around data protection and the GDPR. This includes:

10.1 Having appropriate contracts in place when outsourcing functions that involve the Processing of Personal Data (see section 11 below).
10.2 Implementing appropriate security measures.
10.3 Maintaining records of the Data Processing that is carried out across UUSU.
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 legislation.

11. Use of Personal Data by Processors

Where a Processor including for example, consultants or contractors are engaged by UUSU on work that requires the Processing of Personal Data, UUSU 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 UUSU uses a Processor it must have a written contract in place along with any appropriate data sharing agreements. Processors must only act on the documented instructions of UUSU 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 organisations 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-77right-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 UUSU in accordance with the GDPR. A complaint may be submitted in writing to the Data Protection Officer, David Longstaff, CEO and Data Protection Officer, c/o UUSU, University of Ulster, Room 11H03, Jordanstown Campus, Shore Road, Newtownabbey BT37 0QB or by email at: d.longstaff@ulster.ac.uk. Alternatively, a complaint may be made to the Office of the Information Commissioner. Full particulars of the GDPR including contact details may be found at: https://ico.org.uk/make-a-complaint/.

14. Policy Implementation

UUSU 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 additional sources of further information on the GDPR are below:

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

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

APPENDIX 1

Current Data Protection Officer Contact

Data Protection Officer:

- Mr David Longstaff
- Telephone Number: (028) 9036 6053
- e-mail: d.longstaff@ulster.ac.uk

APPENDIX 2

Current Records Retention & Disposal Policy

A Records Retention and Disposal Schedule is essentially a table that describes the length of time each business document or record will be retained and its final disposition (disposal or storage). The basic components consist of:

- A description of each type of record which the organisation generates
- A retention period for each type of record

A Records Retention Schedule is an essential component of an effective records management programme. It sets out an organisation's policy on retention of its business records. This provides a basis for consistent action across the entire organisation and eliminates the need for individual employees to make decisions about the retention of the records which they produce or receive during their work. The scope of the schedule is the entire organisation of UUSU.

Record Type	Retention Period
Access to Work Personnel Files	Retain for duration of employment + 3 years
Accident reports	Retain until last action on accident + 1 year
Advice Centre Access	Retain from outcome date + 6 years
Balanced Scorecard reports	Retain for current year + 3 years
Bullying and Harassment Investigations	Retain from outcome date + 6 years
Committee papers	Retain for life of committee + 6 years
Companies House Information	Retain for life of company + 10 years
Corporate Business Continuity Plan	Retain until superseded + 1 year
Criminal Record Checks	Retain from received date + 6 months
Disciplinary Action	Retain from date of action + 6 years
DPA Subject Access Requests	Retain from last action on request + 3 years
Election papers	Retain until termination of appointment + 3 years
Employee expense records	Retain for current financial year + 6 years
Employee Personal File (Which will include all application form, references, contract, any contractual changes, changes to personal information (name, address, next of kin etc) and changes to salary point)	Retain until end of appointment + 3 years
Employer pension contribution records	Retain from end of employment + 13 years
Staff exit questionnaires	Retain from termination of employment + 6 years
External representation	Retain until superseded + 5 years
Financial planning and forecasts	Retain for current financial year + 5 years
Financial Statement records	Retain for current year + 6 years
FOI request	Retain from completion + 3 years
Health and Safety risk assessments	Retain until superseded + 10 years
ICO notification of data controller	Retain from current calendar year + 1 year
Internal and external audit reports	Retain from completion of audit + 5 years
Invoice records i.e. mileage claims / receipts	Retain for current financial year + 3 years
Licenses and contracts	Retain until termination of contract + 6 years
Management Accounts	Retain for current financial year + 3 years
Marketing Materials	Retain for lifespan + 20 years

Monitoring files (Which will include equal opportunities questionnaires returned by the applicants, the Applicant Register and the Recruitment Summary Record).	Retain until end of appointment + 3 years
MoUs and agreements	Retain until termination of contract + 12 years
Payroll records	Retain for current tax year + 3 years
Policies and Procedures	Retain until superseded + 5 years
Purchase Ledger records	Retain for current financial year + 6 years
Purchase orders	Retain for current financial year + 6 years
Recruitment Files (Which will include a copy of the approval to recruit, the job description and personnel specification, the advertisement, all applications received, shortlisting report and all interview records)	Retain until end of recruitment process + 1 year
Risk Register	Retain until superseded + 3 years
Sales Ledger records	Retain for current financial year + 6 years
Service Level Agreements	Retain for duration of contract + 1 year
Sick Leave	Retain for duration of employment + 1 year
Staff Disability Disclosure Forms	Retain for duration of employment + 3 years
Staff Grievances	Retain from outcome date + 6 years
Staff Surveys	Retain until completion of survey + 10 years
Staff training records	Retain for employment + 3 years
Steering group papers	Retain for life of steering group + 6 years
Student Access NI documents	Retain until end of appointment + 6 years
Successful tenders	Retain from end of contract + 6 years
Surveys	Retain anonymised full data set + 10 years
Unsuccessful tenders	Retain from award of supply contract + 1 year
UUSU Officer Alumni	Retain for duration of relationship + 1 year
VAT return records	Retain for current financial year + 6 years
Volunteer Information	Retain for duration of engagement + 3 years
Working group papers	Retain for life of working group + 6 years

APPENDIX 3

UUSU Breach of Data Security – Report Form

Name:	
Address:	
Telephone:	Email:
(A) Please tick as appropriate:	
I am a registered student: YES/NO	My registration number is:
I am a member of staff: YES/NO	in the Department of:
I am not a staff member or student: YES/NO	My association with the UUSU consists of:
B) What do you want to complain about/make UUSU aware of?	
C) Details of your complaint/observations?	
D) When did you first become aware of this?	
E) Have you reported your complaint to anyone else in UUSU?	
F) Supporting Documents - Please attach any supporting documentation	
Signed:	Date:

When completed this form should be returned to David Longstaff, CEO and Data Protection Officer, c/o UUSU, University of Ulster, Room 11H03, Jordanstown Campus, Shore Road, Newtownabbey BT37 0QB. A copy of the Report Form can be emailed to Mr Longstaff at: d.longstaff@ulster.ac.uk.