

 **Data Protection Policy**

(in line with the new legislation: **General Data Protection Regulation (GDPR)**) Date of publication: June 2018

# Introduction

This policy applies to all staff who handle or have access to personal data.

There are a number of reasons why personal data is collected and kept at The Students’ Union, for example about employees, students and other stakeholders.

Through this policy, we aim to ensure that current and future students, colleagues and business partners feel confident that The Students’ Union is a safe and secure place to study, work or do business.

Failure to comply with data protection requirements when handling personal data is breaking the law. This can result in large fines and other legal sanctions. Data breaches can also cause significant distress to individuals and have an adverse impact upon the Students’ Union reputation. It is the responsibility of all staff or others who access or use personal information, to adhere to this Data Protection Policy.

# Purpose

The purpose of this policy is to:

* define the requirements of the General Data Protection Regulation (“GDPR”) as applied by UK Data Protection Legislation in the context of The Students Union at the University West of England;
* clarify responsibilities and duties, and set out the structure within which they will be discharged.

# Scope

This policy applies to all personal information processed by, or on behalf of, The Students’ Union. This includes personal information accessed or used by UWE colleagues, as well as, for example, contractors and consultants.

The formats in which personal data is handled can range from electronic, hard copy, and voice recording formats, to spoken forms of communication.

Personal data is any information that can be attributed to an identifiable individual, including names, email addresses, academic performance and qualifications.

Sensitive personal data or ‘special category data’ includes disability status, sexual orientation, sex life, ethnicity, medical information (both physical and mental health), political, philosophical and religious opinions/beliefs, and details of criminal convictions or allegations. This category of data requires enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls (e.g. a locked filing cabinet).

Other categories of data also require enhanced protection for example, bank details, other financial details and national insurance numbers.

This policy also applies to de-identified (pseudonymised) personal data where individuals can be re-identified from other information e.g. student numbers and staff numbers.

# Rights

All data subjects (an individual to whom personal data relates) have the following qualified rights:

* The right to rectification if the information held is inaccurate or incomplete
* The right to restrict processing and/or erasure of personal data
* The right to data portability
* The right to object to processing
* The right to object to automated decision making and profiling
* The right to complain to the Information Commissioner’s Office (ICO)

In addition, individuals can request access to the personal data held about them.

To access personal data held by The Students’ Union, an GDPR Subject Access Form (appendix A) should be completed and sent to the Data Protection Officer, The Students’ Union, U block, Coldharbour Lane, Frenchay Campus, BS16 QY, by post or by email to Tim.Benford@uwe.ac.uk.

# Obligations

To comply with the law, information must be collected and used fairly, stored securely and not disclosed to any other person unlawfully. This is captured in the data protection

principles set out in the GDPR. Those handling personal data must comply with these principles.

Personal data shall:

* Be obtained, processed and used **fairly, lawfully and transparently**;

Be collected for **specified, explicit and legitimate purposes** and not processed for any other purpose;

* Be adequate, **relevant and limited to what is necessar**y in relation to the purposes for which they are processed;
* Be **accurate** and, where necessary, kept up to date;
* Be **kept for no longer** than is necessary;
* Be **protected** by appropriate security measures to prevent loss or unauthorised access

In addition personal data should not be transferred outside of the European Economic Area. In cases where this may be necessary, please seek the advice of the Data Protection Officer.

Privacy notices and lawful processing

Individuals **must** be provided with Privacy Notices before their personal data is collected or used.

In some cases, University-wide Privacy Notices are already in place for the use of staff and students’ personal data. If you need something beyond this, please seek guidance from the Data Protection Officer and follow the model Privacy Notice template.

Third party data processing

Personal data cannot be processed by a third party unless the third party has been approved and signed on behalf of The Students’ Union and the Data Processor (i.e. the third party). If you need a Data Processing Agreement or any associated advice, please contact the Data Protection Officer.

In certain instances where the relationship around data sharing is more complex it may be necessary to agree a Data Sharing Agreement between the interested parties. Please contact the Data Protection Officer for advice.

Ad-hoc third party requests for personal data (for example from the police) should be referred to the Data Protection Officer.

Data protection by design and default

It is the responsibility of all staff and students to incorporate **data protection by design and default** into all activities, processes or projects that may involve the use of personal data. This includes undertaking a Data Protection Impact Assessment (DPIA) screening assessment, and where appropriate, a full Data Protection Impact Assessment to establish the controls needed for protecting personal data. Methods of control include, for example, encryption, anonymisation and pseudonymisation.

Guidance on conducting Data Protection (Privacy) Impact Assessments (Appendix B).

It is the responsibility of all staff and post-graduate research students to immediately notify Tim.benford@uwe.ac.uk by phone if you become aware that personal data is lost, misused, compromised or stolen. This includes, for example, the loss of a laptop.

Where necessary, the Data Protection Officer will report breaches to the Information Commissioner’s Office (ICO) and notify all individuals affected.

Deliberate misuse of personal data will result in disciplinary action and may lead to criminal prosecution. Examples of misuse include sharing passwords between colleagues, asking a colleague to give you data about a data subject or browsing data through Student Union systems about data subjects. This list is not exhaustive.

# Roles and Responsibilities

The **Board of Trustees** provide senior management oversight of data protection matters at The Students Union.

The **Data Protection Officer** is the designated contact for all matters related to data protection and first point of contact with the regulator (Information Commissioner’s Office).

**All staff** are responsible for adhering to this policy as per the Terms & Conditions of employment.

Appendix A.

**Data Protection Subject Access Request Form**

1. **Personal Details of Data Subject**

**1. Details of the person who the information is about (the data subject).**

Full name …………………………………………………………………………………………………… Address ………………………………………………………………………………………………………

………………………………………………………………………………………………………………….. Telephone Number ………………………… Faculty/School.……………………………..... Student Number/Staff Payroll Number (if applicable) ……………………………………… Name of course (if applicable) ……………………………………………………………………… E-mail Address……………………………………………………………………………………………..

1. **Alternative Contact Details (third parties only)**

Only complete this section if you are **not** the data subject, i.e. you are requesting information on behalf of another person.

|  |  |  |
| --- | --- | --- |
| Title | Forename(s) | Surname |
| Address | Telephone number |
| Email address |
| Relationship to data subject/authority for making request |

1. **Records Required**

**(PLEASE COMPLETE ALL SECTIONS)**

* 1. **Please tick the category/categories into which your enquiry falls**

|  |  |
| --- | --- |
| Category |  |
| Sports Associations or Community Associations |  |
| Student records |  |
| Disciplinary records |  |
| Grievance records |  |
| Other HR related documents |  |
| Health and medical matters |  |
| Political, religious or trade union information |  |
| Personal details, e.g. name, address and date of birth |  |
| Other (please specify or describe if possible) |  |

* 1. **Please describe the information you seek in as much detail as possible. This will help us to identify the information you require.**
	2. **Sections / Departments to search**

**Please tick below which (if any) of the following sections/departments the documents you are seeking may be found or which you would like us to search.**

|  |  |
| --- | --- |
| Service / Department | Search () |
| Your Community or Sports Association |  |
| Human Resources |  |
| Student & Representation Services |  |
| Commercial Services |  |
| Finance |  |
| IT Services |  |
| Marketing |  |
| Student Services  |  |
| Facilities  |  |
| Other(s) (please specify) |  |

1. **Identity**

If you are requesting personal data of which you are the subject you must supply:

* a photocopy/scan of proof of your identity with this form, such as passport, driving licence or University ID card.

If you are requesting personal data on behalf of a subject you must describe your relationship to the subject and supply:

1. written signed authority of the subject, and,
2. a photocopy of proof of the subject’s identity with this form, such as passport, driving licence or University ID card.
3. **Declaration**

I certify the information provided in this form is accurate to the best of my knowledge. I accept that The Students’ Union will take reasonable steps to establish identity prior to release of personal data.

I request that The Students’ Union at the West of England provide me with a copy of personal data relating to the subject named in Section 1 of this form.

I enclose the following:

* A photocopy of the data subject’s proof of identity;
* Written and signed authority of the data subject (third parties only).

|  |  |  |
| --- | --- | --- |
| Signed---------------------------------- | Please print name---------------------------------- | Date--/--/---- |

**Please return the completed form either via e-mail marked clearly “Data Subject Access Request” to the following e-mail address:** **Tim.Benford@uwe.ac.uk****.**

**Alternatively, send by post to the following address:**

The Students’ Union

U Block

Frenchay Campus

Coldharbour Lane

Bristol BS16 1QY

Appendix B.



**Data Protection Impact Assessments**

A Data Protection Impact Assessment (DPIA) should be completed at the outset of any project, or change to an existing system or process, that involves or may involve the collection or handling of personal information that is considered high risk. It identifies risks to individuals' privacy rights and/or corporate risks (such as failure to comply with relevant data protection legislation), and where relevant identifies measures required to mitigate those risks.

In order to decide whether it will be necessary to conduct a DPIA you must consider the following screening questions:

* Will the project or process involve the collection of new information about individuals?
* Will the project or process compel individuals to provide information about themselves?
* Will information about individuals be disclosed to individuals or organisations who have not previously had routine access to the information?
* Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
* Does the project or process involve you using new technology that may be perceived as being intrusive such as the use of biometric technology?
* Will the project or process result in you making decisions or taking action against individuals in ways that can have a significant impact upon them?
* Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations e.g. health records, criminal records or any other information individuals would consider to be private?
* Will the project require you to contact individuals in ways they may find intrusive?

DPIAs are strongly recommended by the Information Commissioner's Office. From May 2018, DPIAs will be mandatory where the personal data processing is considered to be "high risk".

Further guidance is also available from the [Information Commissioner's Office](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) (external link).

 Examples of where a DPIA must be considered

* Implementation of new systems or projects that process high volumes of personal data, such as HR Online and student records system.
* Systems or projects that process particularly sensitive personal information (e.g. concerning health).
* Third parties processing high volumes of personal data or any sensitive personal data on behalf of the University.
* Processing of personal data that could be considered 'profiling' of individuals (e.g. learning analytics).
* Any automated personal data processing that results in decisions being made about individuals without human input
* Processing perceived to be particularly intrusive (e.g. CCTV).
* Processing personal data involving children or vulnerable adults.
* Where a contract/agreement or grant requires us to conduct a Data Protection Impact Assessment.
* Any processing of biometric data, such as fingerprints or face recognition

# Review

This policy shall be reviewed annually, or more frequently if appropriate, to reflect relevant legislative, regulatory, or organisational developments.