UWE Data Protection Policy

(in line with the new legislation: **General Data Protection Regulation (GDPR)**)

Date of publication: May 2018
Version: 0.7

Introduction

This policy applies to all staff and postgraduate research students who handle or have access to personal data.
There are a number of reasons why personal data is collected and kept at UWE Bristol, 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 University 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 University's 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 University of the West of England;
- clarify responsibilities and duties, and set out the structure within which they will be discharged.

It should be noted that until 25 May 2018, the University shall remain subject to the requirements of the Data Protection Act, 1998 ("DPA"). From 25 May 2018, UWE will be subject to the GDPR and any other Data Protection legislation applicable in the United Kingdom.

Scope

This policy applies to all personal information processed by, or on behalf of, the University. This includes personal information accessed or used by UWE Bristol staff, as well as, for

example, contractors, consultants and postgraduate research students engaged in UWE-led research.
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 University, an access to personal data form (PDF) should be completed and sent to the Data Protection Officer, Frenchay Campus by post or by email to dataprotection@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 Data Processing Agreement has been approved and signed on behalf of the University by Commercial Services 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.

Further information about sharing personal data with third parties is available here (UWE staff only).

Data protection by design and default

It is the responsibility of all staff and post-graduate research 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 is available on the intranet (UWE Staff only): https://intranet.uwe.ac.uk/tasks-guides/Guide/data-protection#part5

Personal data breaches

It is the responsibility of all staff and post-graduate research students to immediately notify the IT Service Desk by phone if you become aware that personal data is lost, misused, compromised or stolen. This includes, for example, the loss of a laptop. Further details about this process are available here (UWE staff only).

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 UWE systems about data subjects. This list is not exhaustive.

Roles and Responsibilities

The **Directorate** provide senior management oversight of data protection matters at the University, with a reporting line through to the Board of Governors.

Faculty Pro Vice-Chancellor / Executive Deans and Directors of Professional Services also have oversight of data protection and are accountable for their faculties and professional services.

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

Data Protection Liaison Officers are a network of contacts in individual faculties and professional services that support the Data Protection Officer in fulfilment of her/his duties.

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

Contact details for the Data Protection Officer are:
James Button
Data Protection & Records Management Officer
(0117) 932 83029
James2.Button@uwe.ac.uk

Policy owner

For information about this policy or data protection in general please contact:
James Button
Data Protection & Records Management Officer
(0117) 932 83029
James2.Button@uwe.ac.uk

Approval date

22 May 2018

Review

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

Related policies

- Information Security Policy
- Information Handling Policy
- Acceptable Use Policy
- Remote Access Policy

Related procedures

- Data Breach Reporting Steps (UWE staff only)
- Data Breach Procedure (for use by UWE Data Protection Officer and Data Protection Liaison Officers)
- UWE Internal Data Protection Guide / Manual (for use by UWE Data Protection Officer and Data Protection Liaison Officers)