Edge Hill University

Data Protection Policy

Document Title	Data Protection Policy v2.2
Document Owner	SPPU
Approved By	Information Strategy Group
Date of Publication	November 2017
Date for Review	October 2019

1. Introduction

1.1 The University needs to keep certain personal data, for example about its staff and students, to fulfil its purpose and to meet its legal obligations to funding bodies and government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the University must comply with all principles set out in the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR).

1.2 The General Data Protection Regulation requires the University to process personal data under six principles. The principles are similar to those of the Data Protection Act 1998, with added detail at certain points and a new accountability requirement. The principles include:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is compatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be compatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure the personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for long periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical purposed or statistical purposes subject to implementation of the appropriate technical or organisational measures required by the GDPR in order to safeguard the right and freedoms of individuals;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.3 Article 5(2) requires that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles. “The University and its entire staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the University has developed this Data Protection Policy.

2. Status of the Policy

2.1 This policy has been approved by the University’s Board of Governors and any breach will be taken seriously and may result in more formal action.

2.2 Any member of staff or student who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with their Head of Department or the University Data Protection Officer in the first instance.

3. Notification of Data Held and Processed

All staff, students and other users are entitled to:

- Ask what information the University holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed what the University is doing to comply with its obligations under the 1998 Data Protection Act and the General Data Protection Regulation.

4. Responsibilities of Staff and Students

4.1 All staff and students are responsible for:

- Checking that any personal data that they provide to the University is accurate and up to date.
- Informing the University of any change to information which they have provided, e.g. changes of address.
- Checking any information that the University may send out from time to time, giving details of information that is being kept and processed.

If, as part of their responsibilities, staff collect information about other people (e.g. about students course work or personal circumstances, or about members of staff in their department or research group), they must comply with the Policy and with the Data Protection Guidance Notes.

4.2 Students who use the University computer facilities may, from time to time, process personal data. If they do so, they must notify their head of department who will inform the University Data Protection Officer.

5. Data Security

5.1 The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Detailed advice on data security can be found in the University Information Security Policy; a brief guide can also be found in the Data Protection Breach Guidance Notes.

6. Rights to Access Information

6.1 Staff and students and other users of the University have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. Any person who wishes to exercise this right should make the request in writing to the University's Data Protection Officer, using the standard Subject Access Request Form. The University will make a charge on each occasion that access is requested.

6.2 The University aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month of receipt of a completed form unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

7. Publication of University Information

7.1 Information that is already in the public domain is exempt from the Act and the GDPR. This would include, for example, information on staff contained within externally circulated publications such as the University's Annual Report. Any individual who has good reason for wishing details in such publications to remain confidential should contact the University Data Protection Officer.

8. Subject Consent

8.1 The need to process data for normal purposes is communicated formally to all staff through the contract of employment, and to students at registration. In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data must be obtained. Processing may be necessary to operate University policies, such as health and safety and equal opportunities.

9. Retention of Data

9.1 The University will keep some forms of information for longer than others. The University has a Records Retention Schedule, which can be obtained via the web at www.edgehill.ac.uk/governance/strategies-policies/.

10. Edge Hill Student Union

10.1 The Edge Hill Students Union (EHSU) is a separate legal entity from Edge Hill University and therefore a separate data controller. The University shares student personal data with EHSU in order for the Union to administer membership of EHSU and its clubs and societies, to communicate with members, to hold elections of officers, to ensure the safety and security of members (including identification of individual members), to provide welfare services, to market services provided directly by EHSU and to analyse EHSU service provision and membership needs.

11. Use of CCTV

The University's use of CCTV is regulated by a separate Code of Practice. Edge Hill University has in place and is further developing its CCTV surveillance system, for reasons of personal security and to protect University premises and the property of staff and students.

CCTV images if they show a recognisable person are personal data and covered by the Data Protection Act. This Policy is associated with Edge Hill University CCTV Policy.

12. Notification to the Information Commissioner's Office (ICO)

12.1 The Act specifies arrangements for the notification of processing undertaken by the University. The University has a wide-ranging notification, which can be accessed online, reference number Z5265461. Any member of staff who is uncertain as to whether their activities are included in the University's notification should contact the Data Protection Officer in the first instance.

12.2 The Act obliges the University to provide a complete description of all personal data – its use, purposes, disclosures and sources – to the Information Commissioner, and imposes criminal liability where obligations are neglected. The University notifies the ICO of its personal data processing activities annually. The notification process includes informing the ICO of the following:

- The purpose for which the University processes personal data
- The types of individuals (data subjects) to whom this personal data relates
- The types of data (data classes) processed
- The individuals or organisation to who this personal data is disclosed, or intended to be disclosed
- The countries or territories outside of the European Economic Area, if any, to which personal data is transferred, or intended to be transferred.

Staff must only process personal data for the purposes listed within the University's current notification. Processing undertaken outside the University's notification is unlawful.

13. The University's Designated Data Controller

13.1 Further information, including Frequently Asked Questions and Guidance, can be found on the University's Information Governance Intranet site.

The University is the data controller under the Act and is therefore ultimately responsible for implementation. However, day-to-day matters will be dealt with by the University Data Protection Office, dataprotection@edgehill.ac.uk. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the University Data Controller.

Document Owner and Approval

Edge Hill University is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff on the Wiki Page.

This policy was approved by the Information Strategy Group in March 2015 and is issued on a version-controlled basis.

Change History Record

Version	Description of Change	Approval	Date
1.0	Initial Draft	-	
1.1	Minor comments and corrections	-	
1.2	Updated v1.2 protected from amendment	-	
2.0	Principle and Consent Update	ISG Board	April 2015
2.1	None	-	March 2017
2.2	GDPR Compliance Update	ISG Board	November 2017