Edge Hill University

Data Protection Policy

Document Title	Data Protection Policy v2.5
Document Owner	SPPU
Approved By	Information Strategy Group
Date of Publication	February 2020
Date for Review	January 2022
Document Status	Active

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 2018 (DPA) and the General Data Protection Regulation (GDPR). This is one of a suite of policies that aims to ensure the University is compliant with GDPR and has a robust Information Governance framework.

1.2 The GDPR introduces strengthened right for individuals, greater sanctions for breaches and an accountability requirement for data controllers to demonstrate compliance and robust governance. The data controller decides on the nature, scope, context and purpose of processing the data whereas a data processor acts only on instruction from a data controller and processes data on behalf of the data controller. The University is a data controller and, in some instances, may be a data processor.

1.3 The General Data Protection Regulation (GDPR) places restrictions on what the University can do with personal data; certain conditions, which include obtaining data subject consent in some instances, must be met before processing can take place. The term processing covers almost anything that is done to data by reference to individuals and the practical implications of these restrictions are wide-ranging. The GDPR requires the University to process personal data under six principles. The principles are similar to those of the Data Protection Act 2018, 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.

1.4 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

The main data the University processes is:

- Staff Data
- Student Data
- Research Data
- Third Party Data

All staff, students and other users are entitled to the right to be informed of the following:

- The identity and contact details of the data controller.
- Purpose of the processing and the legal basis
- Any recipients of the data
- Details of transfers to third country and safeguards
- Retention period
- The right to lodge a complaint
- The existence of any automated decision making

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

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.

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 30 calendar days 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.

6.3 Individuals are entitled to receive their data in a structured, commonly used and machine readable format so it can be transmitted automatically to another data controller. This applies only to information that has been originally provided by the individual themselves and is being processed by automated means for the purpose of a contract.

7. Right to Erasure / Be Forgotten

In certain specific circumstances individuals can request deletion of their data. It is to be recognised that the instances where this right will apply to data processed by the University will be very few as the University has a legal obligation to retain a central record of all staff and students.

8. Publication of University Information

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.

9. Personal Research Data

Staff are responsible for applying this policy to any personal data they acquire during research studies undertaken by themselves or by students under their supervision. Any staff or student research project that collects personal data from participants in the study must have formal ethical approval before it begins. Participants must be informed on how the data being collected will be stored, preserved and used int eh long erm, and give their

consent to this use of their data. Personal data collected during research studies should be held, where appropriate, in a fully anonymised form that protects the confidentiality of its participants.

10. Subject Consent

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.

11. Retention of Data

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 https://go.edgehill.ac.uk/display/compliance/Information+Governance+Guidance+and+Policies

12. Edge Hill Student Union

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.

13. 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.

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

14.1 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.

14.2 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.

15. Data Breach Notification

One of the requirements of current Data Protection legislation is that, by using appropriate technical and organisational measures, personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Article 4(12) of the GDPR defines a "personal data breach" as:

"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"

Data security breaches should be reported immediately to the Data Protection Office. The Data Breach reporting form (Appendix 1) should be completed in all instances. The Data Protection Office will keep a log of this information. Further information regarding suspected breaches of personal data can be found in the University Data Security Breach Policy.

16. Legitimate Interests

The need to proves data for normal purposes has been communicated to all staff, in employee contracts and to students during induction and registration and in student contracts. In some cases, if the data is sensitive for example information about health, race or gender, express consent to process data must be obtained. Processing may be necessary to operate University policies, such a health and safety and equal opportunities.

17. Third Party Providers

The University contracts with third parties certain functions that involve the processing of personal data. It is a requirement in these circumstances for a written contract to exist between the University and the third party which specifies what processing the third party is authorised to undertake on behalf of the University and action the third party must take in the event of a security breach or a subject access request.

18. The University's Designated Data Controller

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.

Appendix 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If a breach is discovered, please notify the Head of Department/School immediately, complete Section 1 of this form and email it to the Data Protection Officer (dataprotection@edgehill.ac.uk).

Section 1: Notification of Data Security Breach	**To be completed by HOD of the person reporting the incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Lead Investigation Officer in consultation with the Head of area affected by the breach**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • Special categories personal data (as defined in the Data Protection Legislation) relating to a living, identifiable individual's a) racial or ethnic	

origin; b) political opinions or religious beliefs; c) trade union membership; d) genetics; e) biometrics (where used for ID purposes) f) health; g) sex life or sexual orientation	
• Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
• Personal information relating to vulnerable adults and children;	
• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
• Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
• Security information that would compromise the safety of individuals if disclosed.	

Section 3: Action taken	**To be completed by the Data Protection Officer and/or Lead Investigation Officer**
Incident reference number	
Action taken	
Was incident reported to Police?	Yes/No If YES, notified on (date):
Follow up action required/recommended	
For use of Data Protection Officer and/or Lead Officer:	
Notification to ICO	YES/NO If YES, notified on: Details:
Notification to data subjects	YES/NO If YES, notified on: Details:
Notification to other external, regulator/stakeholder	YES/NO If YES, notified on: Details:

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 initially 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
2.3	DPA Compliance Update		April 2019
2.4	Review of processes and guidance	ISG Board	February 2020
2.5	Data Security Breach process clarification	-	June 2020