

Data Protection Policy

September 2022



Edge Hill
University

Contents

Summary	3
Glossary of Terms	3
Purpose	4
Introduction	5
Status of the Policy	6
Notification of Data Held and Processed	6
Responsibilities of Staff and Students	7
Data Security	7
Rights to Access Information	8
Right to Erasure / Be Forgotten	8
Publication of University Information.....	8
Personal Research Data.....	8
Subject Consent	9
Retention of Data.....	9
Edge Hill Student Union.....	9
Use of CCTV	9
Notification to the Information Commissioner's Office (ICO).....	9
Data Breach Notification	10
Legitimate Interests	10
Third Party Providers	11
The University's Designated Data Controller	11
Annexes.....	12
Data Breach Report Form	12
Change History Record	15
Endmatter.....	15

Summary

Data protection legislation sets out rules and standards for the use and handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects') by organisations ('data controllers'). It is based around the notions of principles, rights and accountability obligations. The law applies to organisations in all sectors, both public and private. It applies to all electronic records as well as many paper records. It doesn't apply to anonymous information or to information about the deceased. In order to process personal data, the University must comply with all relevant UK Data Protection legislation. Since 25 May 2018, this includes the UK General Data Protection Regulation (UK GDPR), coupled with the UK Data Protection Act 2018 (DPA 2018), which supplements the GDPR in specific ways. These two pieces of legislation replaced the Data Protection Act 1998 (DPA 1998) and the numerous Statutory Instruments issued pursuant to it. There is also supplementary data protection legislation covering specific topics, such as direct marketing. Whilst the introduction of the UK GDPR strengthens a number of areas of data protection, it can be seen as an extension of data protection rather than a revolution of how data must be used by organisations.

Glossary of Terms

Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data controller: is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by the Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data subject: a natural person whose personal data is processed by a data controller or processor.

Personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data breach: 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.

Privacy impact assessment: a process designed to help organisations identify and mitigate privacy risks associated with proposed data processing activities. *For further information, see the University's Privacy Impact Assessment guidance.*

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not 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.

Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Restriction on processing: the marking of stored personal data with the aim of limiting their processing in the future.

Right of access: entitles the data subjects to have access to and information about the personal data being processed by the data controller.

Special categories of personal data: personal data revealing a data subjects racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership or the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Purpose

Data protection is the fair and proper use of information about individuals. It is part of the fundamental right to privacy and is also about individual's trusting that their personal data is safe and secure when handled by the University. Data Protection training must be undertaken by all Edge Hill staff and the aim of this policy is to provide ongoing support and guidance.

Introduction

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

The UK 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.

The UK 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 UK 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 purposes 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.

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 always follow these principles. The University has developed this Data Protection Policy to support compliance.

Since 1 January 2021, the UK has left the European Union. This has created two significant changes with regards to data protection.

- The UK has now become a “third country” in data protection terms. The UK has been awarded an adequacy decision from the EU, meaning data transfer between the UK and the EU can continue as before. This decision will be reviewed in three years.
- The GDPR is European Union legislation. Since the UK has left the EU, the title of the legislation has changed to reflect the UK’s more withdrawn role in Europe. The legislation is now known as the UK GDPR. Whilst fundamentally the same law, it has now been altered to apply only to the UK and its local laws.

Status of the Policy

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.

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.

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

Responsibilities of Staff and Students

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.

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.

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.

Rights to Access Information

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 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.

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.

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.

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.

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 in the

long term, 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.

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.

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>

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.

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.

Notification to the Information Commissioner's Office (ICO)

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.

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.

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 (Annex 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.

Legitimate Interests

The need to process 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.

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.

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.

Annexes

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:	
<p>HIGH RISK personal data</p> <ul style="list-style-type: none"> • Special categories personal data (as defined in the Data Protection Legislation) relating to a living, identifiable individual's <ul style="list-style-type: none"> 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 	
<ul style="list-style-type: none"> • 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; 	
<ul style="list-style-type: none"> • Personal information relating to vulnerable adults and children; 	
<ul style="list-style-type: none"> • 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; 	
<ul style="list-style-type: none"> • Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals. 	
<ul style="list-style-type: none"> • 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:
Report Findings	

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	UK GDPR legislation and BREXIT update	ISG Board	September 2022

Endmatter

Title	Data Protection Policy
Policy Owner	Planning & Data Protection Officer
Approved by	ISG
Date of Approval	
Date for Review	01/09/2025