Data Protection Policy

Contents

NOTE: This policy has also been published on the University's intranet for those with access to it. It is exactly the same, with the exception of additional links to relevant internal policies, procedures and guidance documents.

Summary of Policy

This policy and other supporting policies, procedures and guidance evidence the Open University's ("the University") commitment to protecting the rights and privacy of individuals (including students, staff and others) by safeguarding their personal data and ensuring that privacy is central to what we do.

Summary of significant changes since last version

This is a new policy, developed to ensure compliance with regard to the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 and related EU and national legislation protecting privacy rights. ("data protection law").

Scope

What this policy covers

As an organisation processing personal information, The Open University is registered with the Information Commissioner's Office (ICO) as a "data controller" (Z5521375). This policy covers the processing of all personal information whose use is controlled by it.

The University also acts as a "data processor", processing personal data on behalf of other data controllers. When it does so, it acts on their instructions and on contractual obligations.

This policy applies to everyone working for or on behalf of the University who obtains, uses, accesses or stores personal data, regardless of their role, grade or type of contract. This includes, but is not limited to, agency staff, volunteers, visiting research and teaching staff and external committee members. It also applies to all students when processing personal data on behalf of the University or as a requirement of their studies.

This policy applies regardless of where the personal data is held, including outside University property and on personally owned equipment.

This policy applies to staff and others working for or on behalf of Open University Student Budget Accounts Ltd (ICO Registration Number Z6827884) and to staff and others working for or on behalf of Open University Worldwide (ICO Registration Number Z5854477).

What this policy does not cover

This policy does not apply to FutureLearn Limited (ICO Registration Number ZA004672) which is a wholly owned subsidiary of The Open University. However, for the purposes of delivering courses through the FutureLearn platform, the Open University and FutureLearn are *data controllers in common*, as defined by data protection law. Data subjects are informed about the sharing of their personal data through the FutureLearn Privacy Policy.

This policy does not apply to Open University Students' Association which is an independent organisation (ICO Registration Number Z6135111).

Status of this Policy

This policy was reviewed by the General Data Protection Regulation Steering Group and the Vice-Chancellor's Executive and subsequently approved by the University Secretary in May 2018.

Introduction

The University is a complex organisation highly dependent on the processing of personal data to carry out its activities and it takes its responsibilities with regard to data protection law very seriously. Personal data is owned by data subjects and the University will fully comply with data protection law in order to ensure their rights, informed by good data governance.

Policy

1. Purpose

1.1 This Policy evidences commitment by the University to ensuring that all those defined by the scope of this policy, process personal data in line with data protection law.

1.2. This Policy aims to

a. Ensure adherence to the data protection principles in all processing of personal data
b. Protect the rights of individual data subjects by applying the principles
c. Outline the roles and responsibilities of all users of personal data
d. Outline the potential consequences of non-compliance with this policy

2. Principles

Personal data will be:

2.1. processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency")

2.2. collected and created for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation")

2.3. adequate, relevant and limited to what is necessary in relation to those purposes ("data minimisation")

2.4. accurate and, where necessary, kept up to date ("accuracy")

2.5 retained for no longer than is necessary ("storage limitation")

2.6 kept safe from unauthorised access, accidental loss or deliberate destruction ("integrity and confidentiality")

The University will ensure additional controls are in place for "special category" (sensitive) personal data.

The University will also ensure that it applies appropriate safeguards to protect the rights and freedoms of data subjects when archiving personal data in the public interest for research, statistical or historical purposes.

3. Data Subject Rights

The University will uphold individual data subject rights, specifically the right to:

3.1. obtain free of charge, confirmation as to whether personal data concerning them is being processed and, if it is, a copy of that personal data

3.2 have their personal data rectified and incomplete personal data completed

3.3 erasure when no longer required or to be forgotten, subject to legal obligations

3.4 object to and restrict further processing of their data until the accuracy of the data or use has been resolved

3.5 data portability where the personal data has been provided by consent or contract for automated processing and the data subject requests that a machine readable copy be sent to another data controller

3.6 not be subject to a decision based solely on automated decision making and processing

We will communicate these rights to data subjects through timely privacy notices.

4. Roles and Responsibilities

4.1 **All Users** of personal data must:

- complete relevant training to support compliance with this policy
- ensure that the personal data they hold in any format (for example: electronic, paper) is kept securely
- not disclose personal data in writing or orally, accidently or otherwise to un-authorised third parties
- keep personal data only for as long as agreed in The Open University Retention Schedule
- regularly check that any personal information they have provided to the University regarding their employment or studies is accurate and up to date
- raise any concerns with the University's Information Rights Team in respect of the processing of personal data
- report losses or un-authorised disclosures of personal data to the Information Rights Team
- co-operate fully with any investigation conducted by the University or the Information Commissioner's Office and implement any necessary improvements following a personal data breach
- support the completion of Subject Access Requests by providing information when requested

The above list is not intended to describe all activities that users of University personal data engage in.

4.2 **IGLOS (Information Governance Liaison Officers)**

- are appointed by their Head of Unit to support the Unit in relation to good data governance and compliance with data protection law
- advise staff in their units on the implementation of and compliance with this policy and associated guidance
- act as the first point of contact for their Unit regarding data protection issues and liaise with the Information Rights Team and Data Protection Officer
- maintain and update the Information Asset Register and other records of processing activities and keep the Information Rights Team informed of changes in the use, storage and security of personal data within their unit
- report any loss of personal data or unauthorised disclosures to their Head of Unit and the Information Rights Team
- provide support in responding to specific data subject requests
- report to their Head of Unit on all matters in relation to data protection law
- provide support in responding to Freedom of Information Requests
- co-ordinate annual information compliance activities for the Unit

4.3 **Heads of Units**:

- have overall responsibility for the processing of personal data and for monitoring compliance within their areas of responsibility
- ensure that all staff in their areas of responsibility undertake training provided by the University
- nominate an IGLO (Information Governance Liaison Officer) to act as first point of contact for the Information Rights Team on data protection issues; keep IGLO contact details up to date; facilitate the activities of the IGLO within their Unit
- ensure that IGLOs are given the opportunity to undertake additional data protection training and attend events organised by the Information Rights Team
- have responsibility for the oversight of the review and updating of the Information Asset Register and other records of processing activities in their area of responsibility

4.4 The **Information Rights Team**:

- provide advice, guidance and training to help staff comply with this policy and related procedures
- publish and maintain University-wide data protection policies, procedures, guidance and other resources
- co-ordinate responses to data subjects exercising their rights
- audit the Information Asset Register
- support the activities of the Data Protection Officer

4.5 The **Information Security Team**:

- is accountable for information security governance, policy, risk and compliance
- is responsible for the implementation of information security controls and measures
- collaborates with the Information Rights Team to manage personal data breaches
- provides specialist information, advice and guidance

4.6 The independent **Data Protection Officer**:

- is involved in a timely manner in all issues which relate to the protection of personal data, informing, advising and reviewing recommendations to policies, procedures, standards and controls
- advises, monitors and audits on all matters with respect to data protection compliance under data protection law
- promotes a culture of data protection awareness to embed privacy by design and default across the University
- is the main contact point externally for matters with respect to data protection
- is responsible for assigning responsibilities to staff involved in data processing operations including awareness-raising and training of staff in processing operations
- monitors and reports to the University Secretary, the Vice-Chancellor's Executive, the Audit Committee and other relevant committees and steering groups

4.7 The **University Secretary**:

- is the Senior Information Risk Owner (SIRO) for the University
- is accountable to The Council for ensuring the University's compliance with data protection law
- is responsible for ensuring the Data Protection Officer and their team have sufficient autonomy and resources to carry out their tasks effectively
- ensures that all data protection matters escalated to them are dealt with in an appropriate and timely manner

4.8 The **Information and Data Steering Group**

- defines, approves and monitors data and information governance, including data protection
- oversees data and information governance policies and procedures, roles and responsibilities, training and all activities designed to embed a culture of good data governance, compliance and best practice

4.9 **The University** has a corporate responsibility as a data controller and when acting as a joint data controller or a data processor to:

- ensure there are appropriate technical and organisational measures are in place so that all processing of personal data is carried out in accordance with data protection law
- hold records evidencing its compliance
- co-operate with the UK supervisory authority, the Information Commissioner's Office, to uphold data subject rights

5. Non-compliance

5.1 All users of personal data are encouraged to seek advice and support as quickly as possible if there is a risk of personal data breach, a suspected breach, a near miss or an actual breach. The Personal Data Breach Procedure should be followed without delay. Our intention is to promote a culture of increased openness and improvement with regard to information security and data protection.

5.2 Any careless or deliberate infringement of this policy or data protection law by users of personal data will be treated seriously by the University and may result in disciplinary action.

5.3 The responsibilities outlined in this policy do not waive personal liability for individual criminal offences resulting from the wilful misuse of personal data under data protection law. These include:

- Unlawfully obtaining, disclosing or retaining personal data
- Re-identifying de-identified personal data without the authority of the data controller or processor
- Altering or deleting personal data to prevent disclosure in accordance with the rights of access to data subjects
- Impeding an officer of the Information Commissioner's Office in the course of their duty

Glossary of Terms

The following terms are defined within data protection law as follows:

1. ‘personal data’ means 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

2. ‘processing’ means 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

3. ‘pseudonymisation’ means 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

4. ‘controller’ means 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

5. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

6. ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data

7. ‘consent’ of the data subject means 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

8. ‘personal data breach’ means 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

9. ‘Supervisory authority' means an independent public authority responsible for monitoring the application of GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the European Union. In the United Kingdom this is the Information Commissioner’s Office

Useful Links

Information Commissioner's Office

General Data Protection Regulations (final legal text)

UK Data Protection Bill (UK Parliament website)

Alternative Format

If you are a member of the public and require this document in an alternative format, please contact the Information Rights Team by email at:
data-protection@open.ac.uk

If you are a student and you require this document in an alternative format, please contact the Student Recruitment team via http://www.open.ac.uk/contact/ (phone +44 (0)300 303 5303), or your dedicated Student Recruitment and Support Centre via StudentHome if you are a current Open University student.

If you are a postgraduate research student, please contact the Research Degrees Team by email at research-degrees-office@open.ac.uk.

Feedback on this Policy

If you have any comments about this policy or have suggestions for how it might be improved or if you wish to contact the University's Data Protection Officer, please contact the Information Rights Team by email at: data-protection@open.ac.uk