DATA PROTECTION POLICY

Document Title	Data Protection Policy
Status	FINAL
Document Number	IR01PO
Classification	Public document
Version	V1.0
Published	September 2022
Review Date	September 2023
Document Owner	Data Protection Officer
Department	Information Rights
Author	Sam Mansfield

CONTENTS

1. SUMMARY

This policy is intended to ensure that personal information is collected and used in compliance with the UK General Data Protection Regulation (the "UK GDPR") and other related legislation.

1.1 Summary of significant changes since last version

This Policy was significantly changed in May 2022 to consolidate information and make reference to the Data Protection Standard.

2. SCOPE

This policy applies to all personal data, including special categories of personal data, processed by the Open University.

This includes all electronic personal data, and any other personal data which has some form of structure or index enabling the relevant information to be located. It applies to data in any medium or format, including but not limited to, data stored on electronic media, transmitted across networks, printed out or written on paper, or spoken over a communications medium (e.g. Cellular). This policy applies regardless of where the personal data is held, including outside University property and on personally owned equipment or in personal accounts.

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, consultants, 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; and anyone who accesses University systems, including suppliers and contractors.

This policy also applies to staff and others working for or on behalf of organisations in the Open University Group.

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

3. INTRODUCTION

The University collects and uses personal data relating to various categories of individuals, including enquirers, students, alumni, informal learners, members of staff, volunteers, research participants, employees of partner and supplier organisations, and anyone who communicates with the University. The purposes for processing this personal data are set out in the University's privacy notices.

The University is subject to the UK GDPR and the UK Data Protection Act 2018, the Privacy and Electronic Communication regulation 2003, and associated legislation. This includes the GDPR and the Republic of Ireland Data Protection Act 2018 by virtue of the University office established in the Republic of Ireland. It is also subject to legislation in other jurisdictions where the OU processes personal data, and to data protection legislation with extra territorial reach where we process the personal data of people in those jurisdictions.

The Open University is registered with the UK Information Commissioner's Office (ICO) as a data controller (Z5521375). OU Student Budget Accounts Ltd is registered under Z6827884, and Open University Worldwide under Z5854477. The Open University is also registered with the Irish Data Protection Commission.

4. PURPOSE

This policy sets out the requirements that must be adhered to when processing personal data, delivering the University's commitment to protecting the rights and privacy of individuals by safeguarding their personal data and ensuring that privacy is central to what we do.

5. DEFINITIONS

Definitions of terms are those used in the UK GDPR.

'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.

'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.

6. POLICY PRINCIPLES

6.1 Data protection principles

The University ensures that personal data is processed in compliance with legislation by setting out rules and processes in the Data Protection Standard. The legislation sets out the following principles that all processing of personal data must adhere to.

Personal data will be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject
- ("lawfulness, fairness and transparency")
- collected and created for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation")
- adequate, relevant and limited to what is necessary in relation to those purposes ("data minimisation")
- accurate and, where necessary, kept up to date ("accuracy")
- retained for no longer than is necessary ("storage limitation")
- kept safe from unauthorised access, accidental loss or deliberate destruction ("integrity and confidentiality")

6.2 Special category data

The University ensures additional controls are in place for "special category" (sensitive) personal data, and personal data concerning criminal convictions. This is because use of this data could create significant risks to the individual's fundamental rights and freedoms.

Special category data is set out in the UK GDPR as follows:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;

- data concerning a person's sex life;
- data concerning a person's sexual orientation.

Personal data relating to criminal conviction and offences includes data about criminal activity, allegations, investigations, and proceedings. It includes information relating to the absence of convictions, personal data of victims and witnesses of crime, data about penalties, and conditions or restrictions placed on an individual as part of the criminal justice process.

The processing of special category personal data, and personal data relating to criminal convictions, must comply with the data protection standard, which sets out specific safeguards for special category and criminal conviction data in order to comply with the principles of the GDPR and UK GDPR.

Processing of data relating to criminal convictions must only be carried out where there is a basis in the legislation to do so.

All processing of special category data must be noted in our Record of Processing Activity, along with the basis for processing it and its retention period.

6.3 Data subject rights

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

- 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
- have their personal data rectified and incomplete personal data completed
- erasure when no longer required or to be forgotten, subject to legal obligations
- object to and restrict further processing of their data until the accuracy of the data or use has been resolved
- 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
- 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.

6.4 Accountability

The University is accountable to the principles above, and so will ensure that

- privacy notices are maintained, to inform individuals as to the purposes and means of processing their information
- where possible, the quality and accuracy of information processed is periodically confirmed, and there are mechanisms for data subjects to update their data.
- personal data is regularly reviewed and destroyed, according to the retention schedule, to ensure that is not held longer than is necessary
- personal data is shared only where is it necessary and appropriate to do so, and that data sharing agreements and data processor agreements are in place where necessary to protect the information

- Appropriate security measures are in place to safeguard personal data, via information security policies and other mechanisms
- Personal data breaches, incidents, and near misses are documented and tracked, and reported to the regulator where necessary
- Data subject rights are fulfilled appropriately, and within the necessary timescales
- Data protection by design is carried out for new activities and where processing changes, including the completion of Data Protection Impact Assessments
- Our personal data processing activities are documented, and regularly reviewed and kept up to date
- The data protection standard is maintained, setting out the specific responsibilities and activities required to maintain compliance
- Overall compliance with the legislation is monitored by the Data Protection Officer

7. RESPONSIBILITIES

All Users of University personal data must:

- Comply with the requirements of the Data Protection Standard, in order to adhere to the data protection principles and protect individuals' rights and freedoms in respect of their personal data.
- Complete relevant training to support compliance with this policy and the associated standard.
- Engage with and follow processes as set out in the Standard in a timely way.

The Senior Information Risk Owner has overall responsibility and authority for risk management relating to personal data in the University. The SIRO is responsible for understanding the impact of risks relating to personal data on The Open University's strategic objectives, and authorising appropriate actions or acceptance. The SIRO is the University's strategic risk owner for information related risks

The University Secretary has been appointed as the SIRO.

The Data Protection Officer is responsible for assessing the compliance of the University, and advising the SIRO and colleagues on compliance risks and issues.

The Information Rights team are responsible for operating the University's compliance processes, including maintaining and communicating policies, fulfilling data subject rights requests, logging and managing personal data breaches, managing accountability documentation, conducting data protection impact assessments, and advising staff on compliance issues.

The Information Security team are responsible for conducting security risk assessments, carrying out vulnerability scans, managing security incidents, maintaining and communicating information security policies, and advising staff on security issues

Heads of Unit/ Information Asset Owners have overall responsibility for the processing of personal data and for monitoring compliance within their areas of responsibility, and as such, are information asset owners. They are responsible for ensuring that the personal data in

their area of responsibility is processed in compliance with the data protection standard. They are also responsible for ensuring that all staff, volunteers, consultants, research students and individuals that are associated with their unit are aware of the policy and standard, have received appropriate training, and have necessary resources and equipment to comply with the Policy and Standard.

Information Governance Liaison Officers are appointed by their Head of Unit to support the Unit in relation to good information management and compliance with data protection law. They must comply with the requirements of the data protection standard, to facilitate compliance with the accountability principle and contribute to overall compliance

8. NON-COMPLIANCE WITH POLICY

In addition to this Data Protection Policy the Data Protection Standard shall be adhered to and applied across all projects, programs, systems and/or initiatives.

Where users cannot adhere to the data protection standard for any reason, an exception should be raised as set out in the standard.

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

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

9. REVIEW AND MONITORING

The Policy will be reviewed annually or wherever necessary as part of legislative or organisational change. This is to ensure that it remains effective and compliant with relevant legislation.

If the Policy is updated then the Standard, as well as all other data protection and privacy documentation, controls and processes must be reviewed, and where necessary, updated, to ensure alignment

The Policy will be reviewed by the Chief Information Security Officer, Chief Data Officer, and People Services; and approved by the Data Protection Officer.

10. USEFUL REFERENCES

These documents will provide additional information

Title
Data Protection Standard
Information security policy set for all staff
Information security policy set for IT, third parties and contractors
Information Asset Register
Record Of Processing Activity
Compliance Training Policy
Compliance Training Standard
Data Protection intranet site
Information and Records Management Policy