Data Protection Policy

Version Number 3.0

Effective from September 2020

Quality and Enhancement Office

Contents

1 Policy statement

The Data Protection Act 2018 (DPA18) and the General Data Protection Regulations (GDPR) (together "the Regulations") are designed to protect personal data and uphold the rights and freedoms of living persons. The GDPR is a European-wide standard that affects organisations worldwide that process personal data about EU citizens.

The University processes (holds, obtains, records, uses, and shares) personal data relating to its current, former and future staff and students; research, academic and industry contacts; contractors, visitors and users of all University services. The University is obliged to meet an individual's reasonable expectations of privacy by complying with existing data protection and privacy law.

The University takes its responsibilities seriously and is committed to compliance with the Regulations. The purpose of this document is to set out the approach to data protection at the University of Salford in order to protect personal data as well as the reputation and security of the University.

The policy sets out:

- how the University complies with the GDPR principles;
- responsibilities and accountabilities for data protection;
- our approach to privacy by design and by default;
- how the University manages data protection and privacy risks, in particular potential or actual personal data breaches.

2 Scope

This policy applies to all personal data and special category data[1] processed by the University and on its behalf, regardless of where the information is located. All staff, students and those acting on the University's behalf who process personal data must be aware of and comply with this Data Protection Policy when carrying out their function.

3 Data protection principles

The GDPR sets out seven key principles that organisations must follow. They are not hard and fast rules, rather the principles set out the spirit of the Regulations. Complying with the principles is key to complying with the Regulations.

Lawfulness, fairness and transparency

The University must have a valid ground for collecting and using personal data. This is known as a lawful basis. The University has identified the lawful bases it relies on to collect and process personal data. The University ensures that we are open with individuals about how their data will be used. Privacy Notices are made available to staff and students and research participants.

Purpose limitation

The University ensures that the purposes of processing are set out from the beginning and provides individuals with information on how their personal data will be used. If the University plans to use or disclose personal data for any purpose that is additional to or different from the originally specified purpose, it will ensure that the new use is fair, lawful, transparent and compatible with the original purpose.

Data minimisation

[1] Special categories of data include information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sex life or sexual orientation, or genetic or biometric data used to uniquely identify an individual

The University ensures that the personal data held is adequate, relevant and limited to what is necessary. The University identifies the minimum amount of personal data needed to fulfil its purpose.

Accuracy

The University takes reasonable steps to ensure that the personal data held is accurate and up to date. There is careful consideration of any challenges to the accuracy of information.

Storage limitation

The University ensures that personal data is not kept for longer than is necessary. The University retention schedule outlines the retention periods for categories of information. Staff should be aware of the retention schedules for the information that they process and ensure that information is not kept for longer than is necessary.

Integrity and confidentiality (security)

The GDPR requires that there be appropriate technical and organisational security measures in place to protect personal data. The University policies, culture, organisational structures and operating environment promote the confidentiality, integrity and availability of the University's information assets throughout their lifecycle from beginning, through use to end of use.

Accountability

The University has appropriate measures and records in place to be able to demonstrate compliance with the accountability principle. This includes recording decisions relating to data sharing, implementing data protection policies and taking a "data protection by design" approach. The University documents its records of processing.

4 Responsibilities of staff and students

All staff (including temporary, contractors and volunteers) and students are responsible for:

- adhering to this policy together with other supporting polices such as the IT Acceptable Use and Information Security Policy;
- ensuring that appropriate technical and practical measures are taken to safeguard personal data held from accidental or deliberate disclosure, loss, damage or destruction;
- checking that any personal data that they provide to the University is accurate and up to date;
- informing the University of any changes to their personal information that they have provided, e.g. change 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;
- ensuring that they only process personal data where they have a lawful basis to do so;
- sharing information only where there is a lawful basis to do so.

The University, as Data Controller, exercises overall control over how and why personal data are processed.[2] The University has a Data Protection Officer who monitors compliance with the Regulations, advises on data protection obligations and acts as a contact point for the Information Commissioner's Office (ICO).

5 Rights of data subjects

A data subject is any person whose personal data is being collected, held or processed. Data subjects have a number of rights in relation to the way we process their personal data. These include:

- the right to be informed about the collection and use of their personal data;

[2] Processing includes holding, storing, deleting, sharing, using data in any way.

- the right of access to their personal data;
- the right to rectification: to have inaccurate personal data rectified, or completed, if it is incomplete;
- the right to erasure, also known as the right to be forgotten;
- the right to restrict processing;
- the right to data portability;
- the right to object to the processing of their personal data (in certain circumstances);
- rights in relation to automated decision making and profiling.

The University ensures that there are procedures in place for the assessment, management and monitoring of all individual rights requests. All individual rights request are managed in line with the Subject Access Policy and Individual Rights Policy.

6 Data sharing

Internal sharing

Personal data may only be shared internally if it is necessary to achieve the purposes for which it was collected for, or other lawful purpose. If there are any concerns or queries, the individual aiming to share the data should consult their line manager or the QEO Information Governance team at foi@salford.ac.uk.

External sharing

Routine sharing: personal data can only be shared with third parties if there is a lawful basis to do so. For routine sharing where there is no contract in place, a data sharing agreement should be approved by the business owner, before any sharing takes place. The agreement needs to outline the purposes for sharing and the expectations for each party's processing of the data.

Ad hoc requests to share: before sharing data it must be established that there is a lawful basis to share the data. This entails checking the identity of the person making the request, ensuring there is a secure means of sharing the data, only sharing the minimum data required, and recording the decision to share and associated and actions. If there are any concerns or queries, the individual aiming to share the data should consult their line manager or the QEO Information Governance team at foi@salford.ac.uk.

International Transfers

The GDPR applies primarily to data controllers and processors located in the European Economic Area. If personal data is transferred outside the EEA, there is a risk that individuals will lose the protection of the GDPR. As such, the GDPR restricts the transfer of personal data outside the EEA unless individual rights and freedoms in respect of personal data are protected in another way as set out in the GDPR Article 46, e.g. by using standard contract clauses.

7 Data retention

Personal data must be kept for no longer than is necessary for the purpose for which it is processed. The University has a Data Retention Schedule detailing how long different types of records should be retained. Some timescales are legal requirements whilst others are according to the needs of the school/professional service or University. If there are any concerns or queries, the individual aiming to share the data should consult their line manager or the QEO Information Governance team at foi@salford.ac.uk.

8 Privacy by design and by default

Data protection is the responsibility of everyone within the University, and effective planning and the adoption of good behaviours prevents many issues arising. By implementing the following initiatives, we

ensure the privacy of every data subject remains a key priority in decision making and in everyday ways of working.

Privacy Forum
The University Privacy Forum considers issues relating to data privacy, protection and security, and information governance.

Training
All staff employed by the University, whether permanent or temporary, must complete data protection training within one month of their start date. Completion of data protection training is monitored and reported as appropriate within the University.

Contractual Requirements of Third Parties

Standard contractual terms and conditions should be in place detailing the obligations for both the data controller(s) and data processor(s). The third party must provide sufficient guarantees on how it will process and protect the data before any data is shared. Third parties processing personal data on behalf of the University are required to provide assurance that staff have received appropriate training.

A template agreement for data processors can be found here.

Where data will be processed by a third country outside of the EEA and not defined as having adequate levels of protection by the EU, additional standard contractual clauses are required.

Data Protection Impact Assessments (DPIA)

A DPIA is a process to help the University identify and minimise the data protection risks of certain processing of personal data. DPIAs must be completed by the Business Owner for all new projects and proposed changes to the way that personal data is processed where there is a high risk to individuals' rights and freedoms.

9 If things go wrong
Risk management

Risks are managed in line with the University's Risk Management Policy. Risks are reviewed and monitored by the Data Governance Strategy Group which is attended by the University Data Protection Officer.

Incident Management

An incident management procedure is in place for the identification, reporting and management of near misses, incidents and serious breaches. This includes containment and recovery, assessment of ongoing risk, breach notification and evaluation and response. Staff are able to report any incidents via the online reporting form on the ServiceNow Portal (university login required).

10 Compliance

Failure to do comply with this policy could result in financial and reputational damage to the University and lead to disciplinary or legal action against the individual.

Remember: protect the University, protect individuals and protect yourself.

11 Support and Escalation

The QEO Information Governance team offers advice and guidance in relation to all aspects of data protection, and can be contacted at foi@salford.ac.uk.

12 Related Documentation

The following documents can be found on the University Policy & Procedure pages University of Salford Policies pages http://www.salford.ac.uk/policies or by following the link below

- Privacy Notices
- Information Security Policy
- Incident Management Procedure
- Records Retention Policy
- Data Sharing Policy
- Subject Access Request Policy and procedure
- Data Protection Impact Assessments Policy

Document Control

Document Control Information			
Revision History incl. Authorisation: (most recent first)			
Author	**Summary of changes**	**Version**	**Authorised & Date**
Legal and Governance		v02.0	
QEO	*Revision of policy to incorporate policy statement, reflect GDPR and Data Protection Act 2018, add responsibilities and rights, insert information on data retention and privacy by design and default, add risk and incident management*	V3.0	

Policy Management and Responsibilities:	
Owner:	This Policy is issued by the Quality and Enhancement Office, which has the authority to issue and communicate policy on Data Protection.
Others with responsibilities (please specify):	All subjects of the Policy will be responsible for engaging with and adhering to this policy.

Author to complete formal assessment with the following advisory teams:	
Equality Analysis (E&D, HR) *Equality Assessment form*	1. *March 2020*
Legal implications (LPG)	*2. N/A*
Information Governance (QEO)	3. *N/A*
Student facing procedures (QEO)	4. *N/A*
UKVI Compliance (Student Admin)	5. *N/A*

Consultation:	
Staff Trades Unions via HR Students via USSU Relevant external bodies (specify)	1. Outcome of consultation with TU on 22.06.20; policies were felt to be appropriate. 2. USSU via Privacy Forum, March 2020.

Review:	
Review due:	July 2021
Document location:	University Policy & Procedure Pages

https://testlivesalfordac.sharepoint.com/sites/QEO/SitePages/InfoGov.aspx

Document Control Information
The owner and author are responsible for publicising this policy document.