**Data Protection &
Information Security Policy**

Table of Contents

[Introduction & Purpose 2](#_Toc513649740)

[Definitions 2](#_Toc513649741)

[Responsibilities 3](#_Toc513649742)

[Students, suppliers and contractors 3](#_Toc513649743)

[Student volunteers 3](#_Toc513649744)

[Union employees 3](#_Toc513649745)

[Union managers and departmental leads 4](#_Toc513649746)

[Data Protection Officer 4](#_Toc513649747)

[Senior Management Team 4](#_Toc513649748)

[Trustee Board 4](#_Toc513649749)

[Compliance 4](#_Toc513649750)

[Respecting Individuals Rights 4](#_Toc513649751)

[Processing Special Categories Of Data 5](#_Toc513649752)

[Subject Access Requests 6](#_Toc513649753)

[Lawful Data Processing 6](#_Toc513649754)

[Children 6](#_Toc513649755)

[Data Breaches & Notification 6](#_Toc513649756)

[Data Protection By Design 6](#_Toc513649757)

[Information Security 7](#_Toc513649758)

[Data Storage 7](#_Toc513649759)

[Policy Monitoring 7](#_Toc513649760)

# **Introduction & Purpose**

The University of Salford Students’ Union (“the Union, “we”, “us”, “our”) is committed to the protection of the personal data of students, employees, suppliers and other individuals whom we might hold information about.

The Union recognises the General Data Protection Regulations and the Privacy of Electronic Communications Regulations as the primary statutory responsibilities relating to data handling and processing.

To this end every individual employee, student volunteer, member, or contractor handling data collected or administered by the Union must take responsibility and due consideration for its appropriate use in line with this policy and the declared processing activities. The specific arrangements for handling, processing and administering data can be found at [privacy](http://www.salfordstudents.com/privacy)

These arrangements apply to all employees and volunteers, and overseen by the nominated Data Protection Officer (CEO) reporting to the Resource, Audit and Risk Committee and USSU Trustee Board. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to Union facilities being withdrawn, or even a criminal prosecution. It may also result in personal liability for the individual.

Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

# **Definitions**

The following terms will be used in this policy and are defined below:

* **Data Subjects** - living individuals about whom we hold personal data.
* **Personal Data -** any information relating to a living person who can be identified directly or indirectly from that information.
* **Data Controllers** - people who, or organisations which, decide the purposes and the means for processing personal data.
* **Data Processors** - any person who processes personal data on behalf of a data controller.
* **ICO** - [Information Commissioner’s Office](http://www.ico.org.uk/)
* **Processing** - activity that involves use of personal data, whether or not by automated means.

Sensitive Personal Data ( “special categories of personal data”)

* + Race or ethnic origin
	+ Political opinion
	+ Religious, philosophical or similar beliefs
	+ Trade union membership
	+ Physical or mental health or condition
	+ Sexual life or orientation
	+ Genetic data
	+ Biometric data; and
	+ Such other categories of personal data as may be designated as “special categories of personal data” under the Legislation.

# **Responsibilities**

When dealing with personal data under GDPR, there are six principles set out and we are required to comply with them as a data controller.

Data should be:

* + processed fairly, lawfully and transparently;
	+ collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes;
	+ adequate, relevant and limited to what is necessary for the purpose for which it is held;
	+ accurate and, where necessary, kept up to date;
	+ not kept longer than necessary; and
	+ processed in a manner that ensures appropriate security of the personal data.

**Students, suppliers and contractors**

Students, suppliers and contractors must ensure that all personal data provided to the Union is accurate and up to date, and that they have read and understood the relevant terms of conditions of engagement with the Students’ Union. They must ensure that changes of address etc are updated on the appropriate systems by contacting the relevant staff detailed in the privacy notices at [privacy](http://www.salfordstudents.com/privacy)

## Student volunteers

Committee members, representatives and other student volunteers may handle personal data to administer their activities and services. Students handling such data are required to have completed the *data protection and information security training course* prior to receiving permission to handle any personal data related to Students’ Union activities and services. When handling personal data students are required to follow the guidance set out in the [*data protection and information security handbook*](USSU%20GDPR%20Data%20Protection%20Handbook.docx) including the reporting of data breaches, respecting the rights of individuals and secure processing procedures.

## Union employees

The Union holds various items of personal data about its employees which are detailed in the relevant privacy notice at [privacy](http://www.salfordstudents.com/privacy). Employees must ensure that all personal data provided to the Union in the process of employment is accurate and up to date. They must ensure that changes of address etc are updated by contacting the relevant member of HR staff.

In the course of day to day working it is likely that staff will process individual personal data. Prior to handling any data staff are required to have completed the ***data protection and information security training course***. In addition to this staff must maintain a current knowledge of data processing best practice through refresher courses and learning available on the Information Commissioner's Office [website](http://www.ico.org.uk/). When handling personal data staff are required to follow the guidance set out in the [***data protection and information security handbook***](USSU%20GDPR%20Data%20Protection%20Handbook.docx).

## Union managers and departmental leads

Union managers and departmental leads must ensure that staff handling data in the course of their roles have conducted the appropriate training, are processing data within the frameworks agreed and following the guidance set out in the [***data protection and information security handbook***](USSU%20GDPR%20Data%20Protection%20Handbook.docx).. Managers are also required to conduct termly audits of their relevant spaces and IT infrastructure to identify weaknesses in information security.

##

## Data Protection Officer

The Data Protection Officer is the Chief Executive at the Union. The Data Protection Officer is responsible for:

* Informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
* Monitoring
* Compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.
* To be the first point of contact for supervisory authorities and for individuals whose data is processed (students, employees, customers etc).

The data protection officer shall be assigned the ussu-gdpr@salford.ac.uk email address

## Senior Management Team

The Senior Management Team (SMT) is required to demonstrate ownership of the Union’s data protection policy and to communicate its values across the Union. This accountability cannot be delegated, however operational aspects of data protection management may be delegated to other levels of management. The SMT must gain assurance that these responsibilities are being fulfilled and to ensure resources are available to fulfil the requirements of this policy and associated procedures.

## Trustee Board

The Trustee Board has overall accountability for the strategy of the Union and is responsible for strategic oversight of all matters related to statutory legal compliance and risk for the Union. The Trustee Board should seek assurance from the SMT that effective arrangements are in place and are working through the Resource, Audit & Risk Committee.

# **Compliance**

## Respecting Individuals Rights

The General Data Protection Regulations sets out a series of rights for individuals. Union employees and volunteers planning data processing activities must record how these rights are addressed. The [***data protection and information security handbook***](USSU%20GDPR%20Data%20Protection%20Handbook.docx). details the rights and the organisation’s standardised processes to meet these individual rights.

## Processing Special Categories Of Data

The Union shall only process special categories of data linked to individuals, such as health data, religious and sexual orientation, with the consent of individuals except for where the disclosure is to preserve life or for legal purpose. This data may be analysed in broad terms where no direct link to an individual can be made.

**Subject Access Requests**

The [***data protection and information security handbook***](USSU%20GDPR%20Data%20Protection%20Handbook.docx) details the procedures on how subject access requests must be handled. As standard, the Union does not charge to comply with access requests and will refuse manifestly unfounded or excessive requests. Any individual or department receiving a Subject Access Request must share this with the Data Protection Officer within 5 working days. The Data Protection Officer shall respond to the request within one month of initial receipt.

## Lawful Data Processing

The Union shall only process data within the law. Where a lawful process has been identified; Union employees and volunteers must make a record of the lawful justification within the privacy notice. The [***data protection and information security handbook***](USSU%20GDPR%20Data%20Protection%20Handbook.docx) details the procedures on how to record the lawful processing justification.

## Children

Union staff and volunteers shall not process data related to any individual aged under 16.

## Data Breaches & Notification

The Union shall adopt processes to detect data breaches including audits and other appropriate processes. Employees and volunteers shall report and investigate data breaches as outlined in the Cyber Incident Response Plan (CIRP) contained within the [***data protection and information security handbook***](file:///%5C%5Cisdads.salford.ac.uk%5CSharedData%5CServices%5CStudents%20Union%5CGDPR%20Documents%5C1.%20Data%20Protection%20Handbook%2C%20Policy%20%26%20Procedures%5CUSSU%20GDPR%20Data%20Protection%20Handbook.docx).

Where an employee, volunteer, supplier or contractor discovers a data breach they must report this to the Data Protection Officer within 24 hours. The Information Commissioner’s Office shall be notified within 72 hours of the breach where there is a risk to the rights and freedoms of individuals such as discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where there is a high risk to the rights and freedoms of individuals they shall be notified directly also. The reporting procedures are detailed in the [***data protection and information security handbook***](file:///%5C%5Cisdads.salford.ac.uk%5CSharedData%5CServices%5CStudents%20Union%5CGDPR%20Documents%5C1.%20Data%20Protection%20Handbook%2C%20Policy%20%26%20Procedures%5CUSSU%20GDPR%20Data%20Protection%20Handbook.docx).

## Data Protection By Design

Employees and volunteers are required to adopt a privacy by design approach to planning data collection and processing. In addition to data collection records, Privacy Impact Assessments (PIAs) and where appropriate Legitimate Interest Assessments (LIAs) shall be be completed prior to any data collection or processing. Details of how to conduct PIA’s and LIA’s are contained within the [***data protection and information security handbook***](file:///%5C%5Cisdads.salford.ac.uk%5CSharedData%5CServices%5CStudents%20Union%5CGDPR%20Documents%5C1.%20Data%20Protection%20Handbook%2C%20Policy%20%26%20Procedures%5CUSSU%20GDPR%20Data%20Protection%20Handbook.docx).

# **Information Security**

## Data Storage

Electronically stored personal data must be stored in an encrypted or password protected form to protect against unauthorised access or processing. Physical representation of data, such as paper forms, must be stored within a locked storage unit. When no longer needed, the e-copies should be deleted and any paper copies securely destroyed.

Vital records for the purposes of business continuity must be protected from loss, destruction or falsification by Union employees or staff, in accordance with statutory, regulatory, contractual, and Union Policy requirements.

The Union has 4 primary platforms for securely storing data online - Google Cloud, Dropbox, University of Salford V Drive and One Voice Servers. Staff and Volunteers are required to store data they handle on one of these platforms only as detailed within the [***data protection and information security handbook***](file:///%5C%5Cisdads.salford.ac.uk%5CSharedData%5CServices%5CStudents%20Union%5CGDPR%20Documents%5C1.%20Data%20Protection%20Handbook%2C%20Policy%20%26%20Procedures%5CUSSU%20GDPR%20Data%20Protection%20Handbook.docx).

Explicit permission from line management must be obtained before removing restricted information, including personal data and confidential information from Union premises. Restricted information processed on portable devices and media must be encrypted. The password to an encrypted device must not be stored with the device.

# **Policy Monitoring**

Compliance with the policies and procedures laid down in this document will be monitored via the Union’s SMT, together with reviews by the Resource, Audit & Risk Committee. The Data Protection Officer is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.