Data Protection and Information Security Policy

Approval Details

Approved by:	Trustee Board	**Date**	
Implementation date:	June 2018		
Review date:	2021		
Manager responsible:	Director of Marketing and Communications – Data Protection Officer		

Contents:

1. Introduction

The University of Plymouth Students' Union ("UPSU", "the SU", "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.

UPSU is registered with the Information Commissioners Office, under the registration number: Z1253305

UPSU 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 role, member, or contractor handling data collected or administered by the UPSU 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 https://www.upsu.com/privacy/

These arrangements apply to all employees and student roles and overseen by the nominated Data Protection Officer reporting to UPSU's Senior Management Team and Audit and Risk Committee. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to UPSU facilities being withdrawn, or even a criminal prosecution.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.

2. Definitions

Data Subjects for the purpose of this policy include all living individuals about whom UPSU holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Data Controllers are organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. .

Data Processors include any person or organisation who process personal data on behalf of a data controller.

Personal Data is information which is stored electronically, on a computer, or in certain paper-based filing systems about a living individual who can be identified from that data or from that data and other available data

Processing is any activity which involves the use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing erasing or destroying it. Processing also includes transferring data to third parties.

Sensitive Personal Data "Sensitive personal data" is information as to a data subject's racial or ethnic origin, political opinion, religious beliefs, trade union membership, sexual orientation or marital status, physical or mental health, offences or alleged offences and information relating to criminal proceedings.

3. Data Protection Principles

Use of data is compliant with the Data Protection Act 1998 and specifically with the 8 data principles that are set out within it:

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes (as above), and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Responsibilities

UPSU employees

UPSU holds various items of personal data about its employees which are detailed in the relevant privacy notice at www.upsu.com/privacy/ . Employees must ensure that all personal data provided to UPSU 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 staff within the HR department.

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 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 at www.ico.org.uk. When handling personal data staff are required to follow the guidance set out in the Data Protection Handbook details of which can be found at www.upsu.com/privacy

UPSU managers

Along with the DPO UPSU managers 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 Handbook. Managers with the DPO are also required to conduct termly audits of their relevant spaces and IT infrastructure to identify possible weaknesses in information security.

Students, suppliers and contractors

Students, suppliers and contractors must ensure that all personal data provided to UPSU is accurate and up to date, and that they have read and understood the relevant terms of conditions of engagement with UPSU. 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 https://www.upsu.com/privacy/

Student Roles

Committee members, representatives, volunteers and other defined student roles may handle personal data to administer their activities and services. Students handling such data are required to have completed the Data Protection Training Course prior to receiving permission to handle any personal data related to UPSU activities and services. When handling personal data students are required to follow the guidance set out in the Data Protection Handbook including the reporting of data breaches, respecting the rights of individuals and secure processing procedures. Details of the training course and handbook can be found at https://www.upsu.com/privacy/

Data Protection Officer (DPO)

The Data Protection Officer is the Director of Marketing and Communications at UPSU. 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 is delegated authority by the Chief Executive to carry out their role with the resources required to be effective in the protection and security of the individual data the organisation handles.

The data protection officer shall be assigned the dataprotection@upsu.com email address

Senior Management Team

The Senior Management Team is required to demonstrate ownership of the Union's data protection and security 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 Senior Management Team 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.

The Board of Trustees

The Board of Trustees 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 Board of Trustees should seek assurance from the Senior Management Team that effective arrangements are in place and are working through the Audit and Risk Committee.

5. Compliance

Respecting Individuals Rights

The General Data Protection Regulations sets out a series of rights for individuals. UPSU employees and student roles planning data processing activities must record how these rights are addressed. The Data Protection and Information Security Handbook details the rights and the organisation's standardised processes to meet these individual rights.

Processing Special Categories of Data

UPSU 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 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

UPSU shall only process data within the law. Where a lawful process has been identified; UPSU employees and student roles must make a record of the lawful justification within the privacy notice. The Data Protection Handbook details the procedures on how to record the lawful processing justification.

Children

Union staff and student roles shall not process data related to any individual aged under 16. In the unlikely scenario that there is a requirement to process data of a child the Data Protection Officer shall be responsible for ensuring the processing is robustly compliant with GDPR standards.

Data Breaches

UPSU shall adopt processes to detect data breaches including audits and other appropriate processes. Employees and student roles shall report and investigate data breaches as outlined in the Cyber Incident Response Plan (CIRP) contained within the data protection and information security handbook.

Where an employee, student role, 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.

Data Protection By Design

Employees and student roles 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 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.

6. 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.

UPSU has two primary platforms for securely storing data online - University of Plymouth Office 365 and Memberships Services Limited (MSL). Staff and Student roles are required to store data they handle on one of these platforms only as detailed within the Data Protection Handbook

Explicit permission from line management must be obtained before removing restricted information, including personal data and confidential information from UPSU 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.

Third Party Contracts

UPSU transfers data to third parties for process in line with guidance contained within the Data Protection Handbook. Prior to data transfer a contract to ensure compliance with relevant legislation must be in place with oversight by the Data Protection Officer.

IT Systems

Employees and Student roles must undertake a Data Protection Training Course to ensure sufficient security awareness. Employees and Student roles must make best attempts to protect their identity by using a strong password. Account passwords and usernames should not be shared without authorisation from organisational managers.

Digital equipment and media containing information must be secured against theft, loss or unauthorised access when outside the UPSU's physical boundaries. In addition, all digital equipment and media must be disposed of securely and safely when no longer required – the Data Protection Handbook outlines the appropriate procedures.

7. Policy Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Union's Leadership Team, together with reviews by the Audit and 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.

END OF POLICY