Data Protection &
Information Security Policy

Introduction

Durham 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. As of 25 May 2018, the General Data Protection Act (GDPR) will become enforceable in all countries within the EU, replacing the Data Protection Act 1998. This policy is designed to help all those to whom the Policy applies to comply with their obligations under the GDPR.

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.

These arrangements apply to all employees and volunteers, and are overseen by the nominated Data Protection Officer reporting to the Union's leadership team and Audit and Risk Committee. 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breach of the data protection policy may lead to disciplinary action being taken, or access to Union facilities being withdrawn, or even a criminal prosecution.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.

Who the Policy applies to

This Policy applies students of Durham University and employees, volunteers, suppliers and partners of Durham SU that we may hold data about, alongside other agents who have a lawful basis to collect or otherwise handle personal data.

The categories of individuals include:

- Students
- Suppliers and contractors
- Student and non-student volunteers

- Union employees
- Union managers and project leads
- The designated Data Protection Officer
- Children

Definitions

This section will introduce key definitions used throughout this document.

Personal Data: Information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Data Controller: The individual who determines the purposes and means of processing personal data, in line with data protection principles.

Data Processors: The individuals who are responsible for processing personal data on behalf of a controller.

Charitable Objects: Objects' describe and identify the purpose for which the charity (Durham Students' Union) has been set up.

Information Commissioner's Office: The UK's independent body set up to uphold information rights.

Data Protection Principles

Anyone processing personal data must do so in accordance with the data protection principles outlined by the Information Commissioners Office

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Additionally, Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Responsibilities

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' Union. They must ensure that changes of address and other personal details are updated on the appropriate systems by contacting the relevant staff detailed in our privacy notices.

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 data protection training prior to receiving permission to handle any personal data related to' Union activities and services. When handling personal data students are required to follow the guidance set out in the data protection guidance 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. 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 finance staff or management.

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 data protection training. 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 our data protection guidelines.

Union managers and project leads
Union managers and project 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 our data protection guidelines. 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, advice 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 has authority to carry out their role with the resources required to be effective in the protection and security of the individual data the organisation handles.

Senior Leadership Team

The Senior Leadership Team 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 Senior Leadership Team must gain assurance that these responsibilities are being fulfilled and ensure resources are available to fulfil the requirements of this policy and associated procedures.

Board of Trustees

The Board of Trustees has overall accountability for the administration 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 Leadership Team that effective arrangements are in place and are working through the Audit and 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. Our data protection guidelines detail 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.

The rights of data subjects

Our data protection guidelines detail the procedures on how subject access, personal data erasure, data rectification, data objection and restriction requests must be handled. This information is also provided to individuals in tailored privacy notices. As standard, the Union does not charge to comply with these requests and will refuse manifestly unfounded or excessive requests. Any individual or department receiving a request must share this with the Data Protection Officer within 5 working days. The data subject's request will be processed within 30 calendar days upon receipt of a fully completed form and proof of identity.

Lawful and Fair Data Processing

The Union shall only process data fairly, and 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. Our data protection guidelines detail the procedures on how to record the lawful processing justification.

In brief, fair and lawful processing entails that unless a relevant exemption applies, at least one of the conditions for processing are met, which include that:

- The individual whom the personal data is about has consented to the processing.
- The processing is necessary: in relation to a contract which the individual has entered into; or because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
- The processing is in accordance with the "legitimate interests" condition.

It is also important that subjects are informed of the basis and purposes of the processing, and this should be done through our privacy notices.

Data must only be processed for the purposes notified to the data subject. Data cannot be transferred outside of the EEA.

Accuracy of Data

Durham Students' Union is committed to ensuring that the personal data held is accurate and kept up to date as required under the GDPR. Durham SU's data systems and processes must be annually reviewed by relevant managers to ensure accuracy checks are in place. Where an employee, volunteer or other data processor becomes aware of personal data that the Union holds becoming inaccurate or out-of-date, they are required to notify the Union's Data Protection Officer. The Data Protection Officer is Gareth Hughes (su.admin@durham.ac.uk).

Children

Union staff and volunteers only process data related to any individual aged under 16 where clear privacy notices for children have been provided, and take extra care to ensure that it is in the interests of the individuals. This includes restricting access and ensuring safeguarding

procedures are in place to identify where children's data may be collected. Where we seek consent to process the data of children under 13, this consent must be provided by a parent in line with our data protection guidelines

Data Breaches

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 Data Breach Reporting Process contained within our data protection guidelines.

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. Additionally, when there is a high risk to the rights and freedoms of individuals they shall be notified directly. The reporting procedures are detailed in our data protection guidelines.

Data Protection By Design

Employees and volunteers are required to adopt a privacy by design approach to planning data collection and processing. Responsibilities and oversight structure is provided in Durham SU Data Protection Matrix, which can be viewed by emailing the Data Protection Officer (su.admin@durham.ac.uk). 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 our data protection guidelines

Consequences of failing to comply

Any deliberate breach of the data protection policy may lead to disciplinary action being taken, access to Union facilities being withdrawn, or even a criminal prosecution. It may also result in personal liability for the individual.

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 four primary platforms for securely storing electronic data – Pickaweb servers, Durham University S Drive, Union Cloud and Advice Pro. Staff and Volunteers are required to store data they handle on one of these platforms only as detailed within our data protection guidelines. Staff and volunteers are permitted to store data they handle outside of one of these platforms only with permission of the DPO.

Explicit permission from a member of the Senior Leadership Team 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.

Third Party Contracts

Occasionally the Union may transfer data to third parties for process in line with guidance contained within our data protection guidelines. 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 volunteers must undertake data protection training to ensure sufficient security awareness. Employees and volunteers must make best attempts to protect their identity by using a strong password which is changed regularly. 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 Union's physical boundaries. In addition, all digital equipment and media must be disposed of securely and safely when no longer required - our data protection guidelines outlines the appropriate procedures.

Policy Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Union's Senior Leadership Team, together with reviews by the Audit and Risk Committee, in the form of an annual Data Protection Report to the committee. The Data Protection Officer is responsible for the monitoring, revision, version tracking and updating of this document on a three yearly basis or sooner if the need arises. Feedback and complaints mechanisms will be made available to all users and reviewed as part of Durham SU process for identifying risks and improvements.

Document History

Policy	Reviewed by:	Date:	Amended by:	Date:
Data Protection & Information Security Policy	Audit & Risk Committee	15 May 2018		