Durham SU Data Protection Policy

Policy Name:	**Data Protection and Information Security**		
Approval Date:	29 April 2025	**To Be Reviewed:**	April 2028
Approved By:	General Purposes Committee		
Related Policies:	Remote Working Device Use Policy		

REVIEW HISTORY			
Date	**Name**	**Signature**	**Notes**
15 May 2018	Audit and Risk Committee		
18 November 2020	Performance and Delivery Committee		
29 April 2025	General Purposes Committee		
17 November 2025	Data Protection Committee		Changes to DPO contact and URLs

DURHAMSU

Contents

INTRODUCTION

Durham Students' Union ("the Union", "the organisation", "we", "us" or "our") is committed to the protection of the personal data of students, employees, suppliers and other individuals whom we might hold information about.

This policy is designed to help all those to whom the Policy applies to comply with all applicable UK and EU data protection legislation in respect of personal data, as well as safeguarding the rights and freedoms of persons whose information we may process pursuant to the UK General Data Protection Regulation 2020 (UK GDPR), the Data Protection Act 2018 (DPA), the Privacy and Electronic Communications Regulations (PECR) and any other applicable legislation. In this document, all such legislation is collectively referred to as 'data protection legislation'.

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 trustees. Any deliberate, negligent, or reckless breach of the data protection policy may lead to disciplinary action being taken, or access to Union facilities being withdrawn, or even a criminal prosecution.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 and for more detailed guidance, see the resources listed on the Information Commissioner's Office website[1].

WHO THE POLICY APPLIES TO

This Policy applies to student group leaders/volunteers, employees, volunteers, suppliers and partners of Durham SU, alongside other agents who have a lawful basis to collect or otherwise handle personal data.

Every individual 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.

DEFINITIONS

This section will introduce key definitions used throughout this document.

Personal Data: any information that identifies, directly or indirectly, a data subject

Data subject: refers to any living person who is the subject of personal data held by the organisation.

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

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

[1] Information Commissioner's Office Guide to GDPR (https://ico.org.uk/for-organisations/guide-to-datahttps://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/protection/guide-to-the-general-data-protection-regulation-gdpr/)

Processing: refers to any action taken in relation to personal data including, but not limited to, collection, adaptation, alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination or deletion, whether by automated means or otherwise.

Special categories of data: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, biometric data (where used for identification purposes), data concerning health, data concerning a person's sex life or sexual orientation

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 Article 5 of the GDPR:

1. **Lawfulness, fairness and transparency**: the Union is committed to processing data lawfully, fairly and in a transparent manner.
   The Union identifies a lawful basis for the data that we process, provides data subjects with a privacy notice to ensure we are being transparent about how we will process their data, and keeps data subjects informed of any changes in the way we process data.
2. **Purpose limitation**: data is collected for specified, explicit and legitimate purposes. The Union does not further process data 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).
   The Union collects data so that it can carry out its work, meet its obligations under law, improve our services, report to contract holders and partners, fulfil any request that data subjects make, personalise services to best meet data subjects' needs and keep track of the impact and quality of the Union's work.
3. **Data minimisation**: the Union is committed to collecting data that is adequate, relevant and limited to what is necessary.
   The Union carries out annual reviews of all methods of data collection, checking that they are still appropriate, relevant, and not excessive.
4. **Accuracy**: personal data is kept accurate and up to date.
   The organisation will assume that information submitted by data subjects is accurate at the date of submission. Data subjects are promptly informed via the privacy notice that they are responsible for ensuring that the personal data held by the organisation is accurate and up to date. If the Union is made aware that the data it holds is inaccurate, we will strive to update the data as soon as possible.

5. **Storage limitation**: the Union is committed to keeping data for no longer than is necessary. 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.
Personal data is retained according to the retention schedule, which can be found in our Record of Processing Activity (ROPA) spreadsheet. When the Union no longer needs it, it disposes, deletes or destroys the information securely.

6. **Integrity and confidentiality**: data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

Additionally, Article 5(2) requires that:

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

RESPONSIBILITIES

Data Protection Officer

The Data Protection Officer is usually the Chief Executive of the Union. The Chief Executive, on advice of the Board of Trustees, may appoint an appropriately qualified external expert to be the Data Protection Officer if this is a better way of securing the needed expertise. Durham SU has an external data protection officer, Angjela Molla from Hope and May Data Protection, who you can contact at su.dataprotection@durham.ac.uk or on 0330 111 0013, with data protection questions or concerns explaining that your query relates to Durham SU. The Data Protection Officer is responsible for:

- Informing and advising the organisation and its employees about their obligations to comply with data protection legislation
- Monitoring compliance with data protection legislation, including managing internal data protection activities, advising on data protection impact assessments, training staff, circulating guidance materials[2] and conducting internal audits.
- Being 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 personal data the organisation handles.

The Management Team

The Management 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,

[2] Information Commissioner's Office guidance for Data Protection Officers (https://ico.org.uk/forhttps://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulationhttps://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/gdpr/accountability-and-governance/data-protection-officers/)

however operational aspects of data protection management may be delegated to other levels of management. The Management 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 Performance and Delivery Committee.

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 e.g. collecting information about members of student groups. 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 this policy including the reporting of data breaches, respecting the rights of individuals and secure processing procedures.

Applicants

In the course of applying for employment with the Union, the Union will gather personal data about those applicants, which will be retained, and ultimately disposed of, in accordance with its retention schedule/privacy notice. Applicants must ensure that all personal data provided to the Union in the process of applying for employment is accurate.

The Union will retain the personal data of applicants in line with its retention schedule/privacy notice, and only insofar as pertains to their existing application.

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. For data protection purposes, Trustees of Durham Students' Union are expected to adhere to the same data protection responsibilities as staff when handling personal data.

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 taken each calendar year, and use of additional resources 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 this data protection policy.

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 this policy. Managers are also required to conduct yearly audits of their relevant spaces and IT infrastructure to identify weaknesses in information security.

The Union assumes information submitted by data subjects is accurate at the date of submission, and promptly informs data subjects via the privacy notice that they are responsible for ensuring that the personal data held by the organisation is accurate and up to date.

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. See below for information about data subjects' rights.

Processing Special Categories Of Data

The Union shall only process special categories of data linked to individuals such as ethnicity, health data, religious beliefs and sexual orientation where a legal basis for processing is identified **and** an appropriate condition under Article 9 of the General Data Protection Regulations can be met. Our Record of Processing Activities (ROPA) records these lawful basis.

The rights of data subjects

The Union is fully aware of the data subject rights described in Articles 15 - 22 of the UK GDPR, and these are listed in the privacy notice.

The data subjects' rights include:

1. The right to be informed
   1.1. Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. The organisation is committed to comply with this right and we do so via the privacy notice.
2. The right of access

2.1. A data subject has the right to make access requests in respect of personal data that is held and disclosed. To understand how we deal with Subject Access Requests, please view our SAR process and template.

3. The right of rectification

3.1. If the data subject becomes aware that the organisation is holding incorrect information about them, they have the right for it to be corrected, and if their information is incomplete, they can also submit additional information to be added.

4. The right to be forgotten (erasure)

4.1. If a data subject asks the organisation to delete their information, as stated in Article 17, the organisation will do so without undue delay when:

4.1.1. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed

4.1.2. the data subject withdraws consent (if that is the basis on which the processing is taking place), and where there is no other legal ground for the processing

4.1.3. the data subject objects to the processing and there are no overriding legitimate grounds for the processing

4.1.4. the personal data has been unlawfully processed

4.1.5. the personal data has to be erased for compliance with a legal obligation

4.1.6. the personal data has been collected in relation to the offer of online services to a child

In addition, if the organisation has made the information public, the organisation must try to have it erased in other locations as well. In conjunction with Article 19 of the UK GDPR, the organisation informs anyone to whom data has been disclosed, unless this 'proves impossible or involves disproportionate effort'. The organisation will also inform the data subject which recipients their data has been disclosed to, if they ask.

There are exceptions to the 'right to be forgotten' for reasons relating to freedom of expression, public health, archiving, research and statistics, legal claims and legal obligation.

There may also be circumstances where the organisation has no choice but to retain data, for example to mark a record for suppression to ensure that no direct marketing is sent to that individual in the future.

The organisation will process a request for erasure without undue delay, and within one month of receipt.

1. The right to restrict processing

1.1. The data subject shall have the right to restriction of processing of their personal data where one of the following applies:

1.2. the accuracy of the personal data is contested by the data subject, for a period enabling the Union to verify the accuracy of the personal data

1.3. the processing is unlawful, and the data subject opposes the erasure of the personal data, requesting the restriction of its use instead

1.4. the Union no longer needs the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims

1.5. the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the Union override those of the data subject

2. The right to data portability

2.1. This right applies when processing is based on consent or a contract between the organisation and the data subject, and the process and the processing is taking place 'by automated means'. It allows data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

2.2. Data subjects are entitled to receive from the organisation a copy of any personal data they have provided in a 'structured, commonly used and machine-readable format', so that they can provide the data to a different controller.

3. The right to object processing

3.1. Data subjects can object to any processing of their data that organisation is carrying out on the lawful basis of legitimate interests. The Union will stop processing if not able to demonstrate 'compelling legitimate grounds'.

4. Rights in relation to automated decision making and profiling

4.1. The Union does not currently undertake automated decision making.

Additional rights of data subjects include:

- The right not to receive direct marketing
- The right to claim damages should they suffer any loss as a result of a breach
- The right to complain and the right to request that the ICO carry out an assessment

If data subjects wish to exercise any rights, they can contact the organisation directly through any of the organisations usual communications channels, including emailing su.dataprotection@durham.ac.uk. They are reminded of their rights and how to exercise them in the privacy notice they receive.

All staff members are trained to recognise an incoming request to exercise any right, to understand when the right applies and to pass it on without delay to the Data Protection Officer immediately, or at least within 5 working days.

All requests from data subjects to exercise any rights should be recorded into the internal log.

Under certain circumstances, mostly described in Schedules 2-4 of the DPA (2018), the organisation may not need to comply with the request by a data subject to exercise one of their rights. Those circumstances will be assessed on a case-by-case basis.

People at Risk

Union staff and volunteers may process data relating to people at risk, and must take extra care to ensure that this processing is in the interests of the individuals. This includes restricting access to data and ensuring safeguarding procedures are in place to identify where the data of people at risk may be collected in line with the Union's Safeguarding Policy[3].

Data Breaches and breach procedure

Article 4.12 of the UK GDPR defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, authorisation, and authorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

The Union shall adopt processes to detect data breaches including contributing to the annual data protection assessment, and other appropriate processes. Employees and volunteers shall report and investigate data breaches as outlined below:

Where an employee, volunteer, trustee, supplier or contractor discovers a data breach they must report this to the Data Protection Officer within 24 hours. The Data Protection Officer and/or staff member will determine actions needed for rectification or to prevent the breach continuing.

The Information Commissioner's Office shall be notified by the Data Protection Officer 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, in line with Durham SU's obligations under the Data Protection Act, 2018[4]. The decision to report such a breach will be made by the organisation. If the breach is reported, the Data Protection Officer will make the report using the ICO's website.

Additionally, when there is a high risk to the rights and freedoms of individuals affected by the breach, they shall be notified directly. In some circumstances, the organisation may decide to not inform the individuals if, in the judgement of the DPO, by doing so it would cause more damage and anxiety to the data subjects than the data breach itself.

If the individuals are informed of the data breach, the organisation will also ask if they want to log a formal complaint to the ICO regarding how their personal data has been managed. If a data subject has been harmed by a breach of data protection legislation, they can take the Union to court for compensation.

The Data Protection Committee (management) will use the breach register to identify lessons the organisation can learn and the changes that can be made – train staff if required to ensure the breach doesn't reoccur.

---

[3] Durham SU's Safeguarding Policy (https://www.durhamsu.com/resources/safeguarding-policy-801e)

[4] Data Protection Act, 2018, Section 67, Subsection 1 (http://www.legislation.gov.uk/ukpga/2018/12/section/67/enacted)

The agreements that the organisation stipulates with data processers includes a clause requiring them to inform the organisation immediately, or in any event within 24 hours of them becoming aware of a breach. This is to allow the organisation to make a report to the ICO within the 72 hours.

Contractors, subcontractors and other parties may be subject to appropriate legal action in accordance with the organisation's processing agreement. If there is a possibility that the breach could amount to a criminal offence, the matter shall be referred immediately to the relevant authorities.

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.dataprotection@durham.ac.uk). In addition to data collection records, Data Protection Impact Assessments (DPIAs) and, where appropriate, Legitimate Interest Assessments (LIAs) shall be completed prior to any data collection or processing. Details of how to conduct DPIA's and LIA's are contained within the templates.

Data Protection Impact Assessments

You should start to fill out the DPIA template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

A DPIA is needed when:

- Starting a large project
- The processing likely to result in a high risk to individuals
- If there is a change to the nature, scope, context or purposes of our processing
- Process personal data that could result in a risk of physical harm in the event of a security breach
- Process personal data in a way that involves tracking individuals' online or offline location or behaviour
- Process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines

A DPIA may need to be considered when processing is to carry out:

- We consider whether to do a DPIA if we plan to carry out any other:
- evaluation or scoring;
- processing of sensitive data or data of a highly personal nature;

- processing on a large scale;
- processing of data concerning vulnerable data subjects;
- processing that involves preventing data subjects from exercising a right or using a service or contract

Legitimate Interest Assessments

The legitimate interest assessment (LIA) template is designed to help you to decide whether or not the legitimate interest basis is likely to apply to your processing. Durham SU recommends it should be used alongside the ICO's legitimate interests guidance.

Assessing legitimate interest means assessing three things.

- What is the purpose for processing the data?
- Is it necessary to process the data (to achieve that purpose)? Ie could it reasonably be done another way?
- How does this balance with the individual's interests?

Consequences of failing to comply

Any deliberate, negligent or reckless breach of the data protection policy may lead to disciplinary action being taken, access to Union facilities being withdrawn. Individuals should be aware that they may even face criminal prosecution by the authorities. 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, and multi-factor authentication should be used where possible. USB devices and external hard drives in particular should be encrypted if possible where personal data is stored on them. 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 primarily uses several platforms for securely storing electronic data – Pickaweb servers, Durham University owned Office 365 platforms, One Voice (our

website) and Freshdesk and Freshworks helpdesk, and a secure Durham University shared drive. Student groups may sometimes use other platforms, particularly Google Drive and guidance and assessment is provided in the student group data protection guidelines to ensure this is done in line with this policy. Staff and Volunteers are required to store data they handle on one of these platforms only as detailed in the guidance to student groups. Staff and volunteers are permitted to store data they handle outside of one of these platforms only with permission of the Data Protection Officer.

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

Data storage

The Students' Union must ensure that data is held securely. Provisions that employees and volunteers must consider putting in place for hard copy data include:

- Lockable filing cabinets
- Clear expectations staff will clear their desks of workspaces of sensitive information or personal data before leaving them
- Secure storage for archived files
- Secure destruction: using a shredder or confidential waste bin Electronic Data

The same requirements apply to electronically held data. Provisions employees and volunteers must consider putting in place include:

Use storage on the University network, or approved platform

- Password protection on all files containing personal data
- Use of the Union's secure platforms for processing data
- Up to date antivirus and malware systems
- Adequate firewalls
- Secure destruction of IT equipment
    - Disposing of IT equipment: Even if you think you've deleted data from your computer it's likely remaining somewhere in some form, so disposing of IT equipment securely is essential. You must contact the Admin Manager to have IT equipment removed and disposed.

Third Party Contracts

Occasionally the Union may transfer data to third parties for processing 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. All third parties we work with who have or may have access to personal data of our data subjects will either comply with this policy, or we will ensure that their data protection policy aligns with this policy.

INTERNATIONAL DATA TRANSFER

Where personal data is stored outside of the UK and the EU, safeguards to protect personal data may include, but are not limited to, the UK Addendum used in conjunction with the EU Standard Contractual Clauses (SCCs), or UK International Data Transfer Agreement (IDTAs). Such safeguards will be subject to Transfer Risk Assessments (TRAs).

IT Systems

Employees and volunteers must undertake data protection training to ensure sufficient security awareness. When accessing or handling personal data remotely, employees must familiarise themselves with and comply with Durham SU's Remote Working Device Policy. 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.

Cookies

The organisations website uses the following types of cookies

Strictly necessary cookies

The following cookies are necessary for the operation of our website and temporarily process a device IP address which is then discarded. Users can disable cookies at any time but this may stop our website from functioning properly for them. Cookies may remain on the users device for up to one year.

- Remember what is in a shopping basket
- Remember progress during an order for a membership, or event ticket
- Remember that a user is a logged in for purchasing a membership, or event ticket, or voting in an election, and that your session is secure

Functional and 1st Party Cookies

Google Analytics

These cookies are used to collect information (non-personal information) about how visitors use our sites. We use the information to compile reports, which will help us to monitor our websites performance and enable us to improve our sites, where necessary. This cookie collects information in an anonymous form, including the number of visitors to our sites, where visitors have come from and the pages they have visited.

Google has developed a plugin for browsers which users can install that helps users to opt out from analytics if they do not wish to use it, and this information should be provided to data subjects in our cookie notice.

Targeting Cookies

Targeting cookies are not in use on our site.

Student Group may also have websites, which use necessary and functional and 1st party cookies.

POLICY MONITORING

Compliance with the policies and procedures laid down in this document will be monitored via the Union's Management Committee together with reviews by the trustees 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.