Data Protection Policy

Policy title	Data Protection Policy
Applicable to	All permanent staff
Date last reviewed	September 2025
Date of next review	September 2026
Owned by	Operations and HR department

1. Purpose of the policy

1.1 The Students' Union is committed to upholding the principles of data protection and ensuring we handle all personal data in accordance with UK law.

This policy explains:

- how we will comply with UK law on data protection
- how we will deal with requests to access personal data
- how employees and contractors can let us know about a potential personal data breach
- what we will do if there has been a personal data breach

This policy should be read alongside our privacy notice Privacy Policy @ University of Sunderland Students' Union.

2. Scope of the policy

2.1 This policy covers the actions that the Students' Union will take in its role as a 'data controller'. UK data protection law determines both the purposes and means of data processing.

Our policy applies to any person or body that handles personal data on the Students' Union's behalf. This includes:

- employees
- agency staff
- contractors
- any third party acting as a 'data processor' for the Students' Union

3. Roles and responsibilities

3.1 Senior managers have overall responsibility for this policy. However, everyone in the Students' Union is responsible for implementing it. To make this happen:

- line managers must ensure their teams comply with the policy
- all staff must complete the GDPR training provide via the University online training platform.
- employees must understand their responsibilities and report any breaches to Louise Dixon, Operations and HR Manager.

3.2 In addition, and to make sure the policy is still accurate and up to date, Louise Dixon Operations and HR Manager will review it once a year.

3.3 In addition, and to make sure the policy is implemented effectively:

- line managers must ensure their team complies with the policy
- employees must understand their responsibilities and report any breaches to is this Operations and HR Manager or Head of Operations

4. Compliance with data protection law

4.1 The Students' Union will comply with:

- the Data Protection Act 2018 (DPA)
- the UK implementation of General Data Protection Regulation (GDPR)

4.2 We will do this by:

- identifying information that we need to treat as personal data or special category data
- applying the data protection principles that are outlined in UK GDPR
- processing personal data in a lawful way

5. Definition of personal data

5.1 Personal data is any information that could be used to:

- directly identify an individual
- indirectly identify an individual, if it is combined with other information

5.2 In cases where personal data is of a sensitive nature, it is classed as 'special category data'. Special category data is information that reveals or concerns an individual:

- race or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data, if used for identification purposes

- health
- sex life
- sexual orientation

6. Application of data protection principles

6.1 The Students' Union will apply data protection principles to any personal data that we process:

- wholly or partly by automated means
- by any other means, and which we intend to add to a filing system

6.2 The data protection principles require that we:

- process personal data in a way that is lawful, fair and transparent
- only collect personal data for specific, explicit and legitimate purposes
- only collect personal data that is adequate and relevant to our business
- take reasonable steps to make sure that data remains accurate
- not keep data for longer than is needed
- make sure that data is processed securely and protected against unlawful processing
- take responsibility for what we do with personal data
- where required, provide evidence that we act according to these principles

7. Lawful processing of personal data

7.1 In addition, the Students' Union will not process an individual's personal data unless at least one of the following conditions has been met:

- we have clear consent from them to do this, and it is for a specific purpose
- we need to do this because of a contract we have with them, or because they have asked us to do so before they enter into a contract
- we need to do this to comply with the law
- we need to do this to protect someone's life
- we need to do this to perform a task that is in the public interest, or because we are acting under official authority
- it is in our legitimate interest to do this, and, on balance, it does not disproportionately interfere with the rights and freedoms of the individual concerned

Also, where the information is special category data, we will only process it if we can identify an additional condition as set out in data protection legislation.

8. Consent

8.1 In cases where we ask for written consent, we will:

- provide this request in an easily accessible format
- use clear and plain language

- not include unfair terms
- make it easy to distinguish the consent declaration from any related content

8.2 In cases where we ask for consent electronically, we will:

- make the request clear and concise
- make sure the request does not cause unnecessary disruptions to our online service

8.3 In all cases, we will not process personal data unless consent was:

- given expressly and freely
- informed, which means the individual understood what they were agreeing to

An individual can withdraw their consent at any time. If they do this, we will stop processing their data immediately.

9. Legitimate interest

9.1 If we believe we can process personal data because we have a legitimate interest, we will:

- complete a legitimate interest assessment
- record the outcome of this assessment

9.2 We will not process the data in question unless we are confident that:

- this is a justifiable use of legitimate interest
- we will be able to demonstrate this using our legitimate interest assessment

9.3 In cases where we process personal data on the grounds of legitimate interest, we will undertake regular reviews of the corresponding legitimate interest assessment. We will do this every 12 – 18 months.

9.4 We will also review a legitimate interest assessment immediately if there are significant changes to the purpose or nature of the processing.

10. Requests to access personal data

10.1 We will ensure any requests to access personal data are handled lawfully.

If the request comes from the person the data relates to (or their authorised representative), we will treat this as a 'subject access request'. We will do this whether we receive the request:

- in writing
- verbally
- on social media

10.2 When we receive a subject access request, we will:

- ensure the person who submitted it is authorised to act on behalf of that person if the person requesting it is not the subject of the data
- if the request is not sent electronically, we will clarify how the requester wishes to receive the information

10.3 We will then consider the arrangements for providing the information. As part of this, we will:

- ensure the data is not subject to a legal exemption or restriction
- ensure that sharing the information will not involve disclosing third-party data
- if need be, ask the requester to clarify their request

10.4 We will provide the requested data within 1 calendar month of the receipt of the request, unless:

- it is subject to a legal exemption or restriction
- we cannot do so without also disclosing third-party data
- we need to extend the response period by up to a further 2 months

10.5 We will only extend the response period in cases where (both conditions apply):

- we need to do so due to the complexity of the request
- we can provide a formal justification for this decision

Where we decide to extend the time limit, we will notify the requester within the initial 1-month period.

If we decide not to comply with the requests or the requester is not satisfied with the outcome, they may ask the Information Commissioner's Office (ICO) to check whether our decisions are correct. The requester will be informed of this when we respond to a request for their personal data.

10.6 We shall also inform the requester:

- the purposes for our processing of their personal data
- the categories of the personal data that we process
- the recipients or classes of recipients to who we disclose the personal data
- so far as it is possible to do so, the period for which the personal data will be stored and the reasons for that storage. Where it is not possible to confirm the storage period, provide the criteria we use to decide that period
- where they are not the source, the sources of any of the personal data that we process
- the existence of automated decision-making
- the right to request correction, removal, restriction or to raise concern in relation to their personal data; and
- the right to lodge a complaint with the ICO

11. Reporting a potential personal data breach

11.1 As part of their responsibilities for helping us implement this policy, all employees, contractors and associated third parties must report potential breaches immediately.

This includes any incidents that involve:

- the sharing of personal data, whether accidental or deliberate, with parties who are not authorised to view it
- the loss or theft of a device that contains, or grants access to, personal data
- attempts by anyone to access personal data by hacking or bypassing IT security measures
- the unauthorised alteration of personal data

Potential breaches should be reported to Louise Dixon, Operations and HR Manager.

12. Actions we will take in response to a personal data breach

12.1 In cases where we believe a breach may pose a risk to someone's rights or freedoms, we will report it to the ICO. We will do this without undue delay and certainly within 72 hours of the issue being raised with us. Where we consider that the breach may pose a high risk to someone's rights and freedoms, we will inform the ICO and the individual(s) concerned.

12.2 If an employee's actions lead to a breach, whether this was deliberate or accidental, they may face disciplinary action. We will take this action in line with our disciplinary procedure.

12.3 If we consider an employee's behaviour to be gross misconduct, this will usually result in dismissal without:

- warning
- a notice period
- payment in lieu of notice

13. How long we keep your data

13.1 We will keep personal data:

- only as long as we need it, and
- in line with:
    - business needs
    - industry standards, and
    - legal obligations.

All documents containing personal data are destroyed securely and in accordance with the data protection principles.