

# Huddersfield Students' Union

Document Title	
<b>Data Protection Policy</b>	
Document Author and Department	Responsible Person and Department
Matthew Short - SLT	CEO All Staff
Approving Body	Date of Approval & Minute Reference
Union Development Committee	09.05.2024 & 06b
Version No	Review Date
5	May 2027
Policy Number	Date of Issue
13	9 <sup>th</sup> May 2024
Document Reference and Path	Purpose of Issue
	Approval and Implementation

## Table of Contents

1	<a href="#"><u>Key terms used in this Policy</u></a>
2	<a href="#"><u>What is this Policy for?</u></a>
3	<a href="#"><u>Who does this Policy apply to?</u></a>
4	<a href="#"><u>What will this Policy achieve?</u></a>
5	<a href="#"><u>Who is responsible for this Policy?</u></a>
6	<a href="#"><u>Lawful Basis for Data Processing</u></a>
7	<a href="#"><u>Individual Rights</u></a>
8	<a href="#"><u>Governance and Accountability</u></a>
9	<a href="#"><u>Data Security</u></a>
10	<a href="#"><u>Data Transfers</u></a>
11	<a href="#"><u>Data Breaches</u></a>
12	<a href="#"><u>Complaints</u></a>

## 1. Key Terms used in this Policy

- 1.1. **GDPR** is the General Data Protection Regulation, which outlines the laws connected to data protection.
- 1.2. **PECR** is the Privacy and Electronic Communications Regulations, which outlines the laws connected to marketing.
- 1.3. **ICO** is the government organisation responsible for delivering and monitoring data protection legislation.
- 1.4. **Privacy statements and notices** are where the Union specifically outlines what data the Union processes, where it is stored, and how long it is kept.
- 1.5. **Data sharing agreement** are agreements between the Students' Union and third parties where data is shared and processed. They outline what can be processed and explicitly define each organisation's responsibilities.
- 1.6. **Freedom of Information** is the legislation about information connected to public bodies such as Universities.
- 1.7. **EEA** stands for European Economic Area which includes all countries in the European Union plus additional countries who are part of the European single market.

## 2. What is this Policy for?

- 2.1. Huddersfield Students' Union is committed to the protection of the personal data of students, employees, suppliers and other individuals whom we might hold information about.
- 2.2. The Students' Union recognises the [UK General Data Protection Regulations](#) (GDPR) and the [Privacy and Electronic Communications Regulations](#) (PECR) as the primary statutory responsibilities relating to data handling and processing. In addition to this the Students' Union shall take guidance from the [Information Commissioners Office](#) (ICO) to ensure it follows the regulations appropriately.
- 2.3. To this end every individual employee, student volunteer, member, or contractor handling data collected or administered by the Students' 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 on the Union website in our [privacy statements](#).

## 3. Who does this Policy apply to?

- 3.1. This policy applies to all employees and volunteers which is overseen by the Students' Union's Senior Leadership Team (SLT), reporting to the Board of Trustees and Union Development Committee. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, and/or access to Union facilities being withdrawn, and/or even a criminal prosecution. It may also result in personal liability for the individual committing the breach.

- 3.2. This policy should be read in conjunction with the [Universities data protection policies and procedures](#) and the Data Share Agreement between the Students' Union and The University of Huddersfield.

## 4. What will this Policy achieve?

- 4.1. In accordance with the UK General Data Processing Regulations (GDPR), the Privacy and Electronic Communications Regulations (PECR), [The Freedom of Information Act 2000](#) and associated legislation, Huddersfield Students' Union has a statutory duty to control and process personal data within specific legal parameters. As such the Students' Union recognises that:
- a) It must process data lawfully, fairly and transparently.
  - b) That data is collected for specified, explicit and legitimate purposes.
  - c) That data is adequate, relevant and limited to what is necessary.
  - d) That data is accurate and kept up to date.
  - e) That data is not kept longer than is needed.
  - f) That data is stored and processed securely.
  - g) It should be able to demonstrate compliance.

## 5. Who is responsible for this Policy?

- 5.1. The **Board of Trustees** have ultimate responsibility for data protection, including that an effective and up to date data protection policy is in place. The Board of Trustees will ensure that the necessary resources are made available for the effective implementation of the policy and are advised on matters relating to data protection by the Senior Leadership Team.
- 5.2. The **Chief Executive Officer** is delegated overall responsibility by The Board of Trustees for data protection and shall be responsible for:
- a) Informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
  - b) Monitoring overall compliance with the GDPR and other data protection laws.
  - c) To be the first point of contact for supervisory authorities and for individuals whose data is processed (students, employees, customers etc).
- 5.3 The **Senior Leadership Team** have responsibility for GDPR compliance and other data protection laws within areas of their control including: -
- a) Ensuring that the Students' Union's Data Protection Policy document is implemented.
  - b) Ensure compliance with the University Data Share Agreement.
  - c) Ensure that sufficient training to staff is delivered.
  - d) Manage data protection risks and ensure operational compliance is monitored.
  - e) Ensuring that data is processed in line with the Students' Union's privacy statements.
  - f) That data is erased within specified time frames.

g) That data breaches appropriately investigated, and changes made to prevent future breaches.

5.4 **Departmental Managers** Have responsibility for data protection and compliance at a departmental level ensuring suitable and sufficient organisational and management arrangements are in place to deliver successful GDPR compliance.

5.5 **All employees and volunteers** shall cooperate with the Students' Union on matters relating to data protection and assist the Students' Union in fulfilling its statutory duty. Any data breach that has taken place directly or indirectly should be reported to the CEO at the earliest convenience.

5.6 **Students** shall take reasonable care of their own data and cooperate with the Students' Union on matters relating to data protection to assist the Union in fulfilling its statutory duty.

5.7 **The University** as outlined in the Memorandum of Cooperation need to share data relating to students and both, as data controllers, are subject to GDPR. Both the University and the Students' Union shall ensure there is always a Data Sharing Agreement in place to govern these arrangements and enable the Union to discharge its objectives.

5.8 The Students' Union may transfer data to **third parties** for processing which will be declared to the individuals whose data is being processed. Prior to data transfer a contract or sufficient privacy statements/policies shall be collected and stored to meet the expectations of the Students' Union privacy statements. All contracts or privacy statements/policies shall include requirements outlined in the GDPR and outlined in guidance from the ICO.

## 6. Lawful Basis for Data Processing

The Students' Union shall ensure it has a valid lawful basis for processing all personal data. There are six available bases for processing to which the Students Union shall select the most appropriate depending on the purpose and relationship with the individual. The Students' Union's privacy statements should include each lawful basis, purpose for processing and retention length.

### 6.1. Consent

There is a high standard for obtaining consent by giving individuals real choice and control.

6.1.1. The Students' Union shall ensure that it provides specific statements of consent that requires a positive opt-in which is separate to other terms and conditions. This shall also include the naming of any third-party controllers who will rely on the consent.

6.1.2. Withdrawal of consent shall be transparent and easy by following information in the Privacy Statements.

6.1.3. Evidence of consent should be retained for reference in line with the retention schedule.

6.1.4. Statements of consent shall remain under consent review, be refreshed to reflect any changes made and individuals kept informed.

6.1.5. Explicit consent shall be used for the processing of special category data.

## 6.2 Contract

- 6.2.1 This legal basis can be used to process personal data to fulfil contractual obligations or because the individual has asked the Students' Union to do something before entering a contract. The processing must be necessary, targeted, and proportionate for the purposes of performing a contract or taking pre-contractual steps.
- 6.2.2 If processing is not necessary for the Students' Union's side of the contract with the individual another lawful basis such as legitimate interests or consent will also be needed to process the data.
- 6.2.3 If processing of a special category is necessary for the contract a separate condition for processing data shall also be needed.

## 6.3 Legal obligation

- 6.3.1 This lawful basis is for the processing of personal data to comply with a common law or statutory obligation.
- 6.3.2 Processing must be necessary to comply with lawful obligations.
- 6.3.3 The Students' Union should be able to identify the specific legal provision or appropriate source of guidance that clearly sets out the obligation.

## 6.4 Vital interests

- 6.4.1 Vital interests can be used as a lawful basis for processing personal data to protect someone's life.
- 6.4.2 If there is another, less intrusive, lawful basis for processing data this basis will not apply.
- 6.4.3 This basis will not apply if the individual is capable of giving consent.
- 6.4.4 If the Students' Union is likely to rely on this lawful basis the circumstances where it will be relevant should be documented.

## 6.5 Public task

- 6.5.1 This lawful basis can be used to process personal data for public functions and powers that are set out in law or to perform a specific task in the public interest that's set out in law.

## 6.6 Legitimate interests

- 6.6.1 Legitimate interests is the most flexible lawful basis for processing.
- 6.6.2 The Students' Union will always use people's data in a way they would reasonably expect, with minimal privacy impact or where there is sound justification for the processing.
- 6.6.3 Processing of data shall follow the three-part test identified by the ICO:
  - a) **Purpose test** – is it a legitimate interest?
  - b) **Necessity test** – is the processing necessary for the purpose?
  - c) **Balancing test** – do the individuals interests override the legitimate interests?
- 6.6.4 Legitimate interests shall always be balanced against an individual's interests, rights and freedoms.

6.6.5 Marketing activities shall also consider whether any consent is required under the [Privacy and Electronic Communications Regulations \(PECR\)](#).

#### **6.7 Special category data**

6.7.1 Special category data is personal data which the GDPR says is more sensitive and therefore needs more protection.

6.7.2 Examples of special category data include race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, sexual orientation.

6.7.3 The students' Union shall only process special category data if the conditions for processing are listed in Article 9(2) of the GDPR are met with legitimate and documented reasons.

#### **6.8 Criminal offence data**

6.8.1 To process personal data about criminal convictions or offences the Students' Union must have both a legal basis and either the legal authority or official authority for the processing.

## **7. Individual Rights**

The GDPR provides the following rights for individuals:

### **7.1. Right to be informed**

7.1.1. The Students' Union will ensure it informs individuals about the collection and use of their personal data including: -

- a) The purpose for processing
- b) The length of time it is retained
- c) Who it will be shared with

7.1.2. The Students' Union will provide privacy information at the time personal data is collected. This information should be concise, transparent intelligible, easily accessible, and use clear and plain language.

7.1.3. When personal data is obtained from a source that is not the individual it relates to the Students' Union will provide the individual with privacy information before the first communication take place or within one month of receiving the data.

7.1.4. Privacy information should be regularly reviewed with any changes being communicated to individuals whose data we hold.

### **7.2. Right of access**

7.2.1. Where possible the Students' Union shall provide access to an individual's data through the Union and University website.

7.2.2. The Students' Union will provide individuals with a simple and transparent process for accessing their personal data and supplementary information. Access information shall be contained in privacy statements and responses shall usually be provided within one month of submitting a request.

7.2.3. If the Students' Union believe a request is manifestly unfounded, excessive, or repetitive a reasonable fee shall be applied to cover administrative costs of providing the information.

### **7.3. Right to rectification**

7.3.1. Where possible the Students' Union will try to keep all data up-to-date and accurate.

7.3.2. Individuals can request for data to be rectified via email.

7.3.3. The Students' Union will respond to all requests within one calendar month.

7.3.4. The Students' Union shall grant and/or refuse rectification following guidance from the GDPR and the ICO.

### **7.4. Right to erasure**

7.4.1. The Students' Union will provide individuals with the right to have personal data erased provided that:

- a) The personal data is no longer necessary for the purpose it was collected for.
- b) Consent was used as the lawful basis for collection and the individual withdraws their consent.
- c) Legitimate interests were used as the lawful basis and the individual objects and there is no overriding legitimate interest to continue the processing.
- d) The processing is for direct marketing purposes and the individual objects to that processing.
- e) Data has been processed unlawfully.
- f) The Union is complying to a legal obligation

7.4.2. The Students' Union shall grant and/or refuse the right of erasure following guidance from the GDPR and the ICO.

7.4.3. The Students' Union shall respond to erasure requests within one month.

### **7.5. Right to restrict processing**

7.5.1. Individuals have the right to restrict the processing of their data by the Students' Union if the following circumstances apply:

- a) The individual contests the accuracy of the data and the Students' Union is verifying its accuracy.
- b) The data has been unlawfully processed and the individual opposes erasure.
- c) The Students' Union no longer needs the data but the individual needs you to keep it to establish, exercise or defend a legal claim.
- d) The individual has objected to the Students' Union processing the data, but we are considering legitimate grounds to override the rights of the individual.

7.5.2. The Students' Union shall grant and/or refuse the right to restrict processing following guidance from the GDPR and the ICO.

### **7.6. Right to data portability**

7.6.1. The Students' Union will ensure that where it's applicable individuals shall be able to obtain and reuse their data for their own purposes across different services.

7.6.2. The Students' Union shall follow guidance from the GDPR and the ICO if an individual requests the transfer of their data.

## **7.7. Right to object**

7.7.1. Individuals have the right to object to:

- a) Processing based on legitimate interests
- b) Direct marketing (including profiling)
- c) Processing for purposes of scientific/historical research and statistics.

7.7.2 HSU shall grant follow guidance from the GDPR and the ICO when fulfilling an individual's right to object.

## **7.8. Rights to automated decision making including profiling**

7.8.1. The GDPR includes specific provisions for automated individual decision making and profiling.

7.8.2. The Students' Union will only undertake solely automated decision making provided that:

- a) It is necessary for entering into or performance of a contract with the Students' Union.
- b) It's based on an individual's explicit consent.

7.8.3. A Data Protection Impact Assessment must be completed to ensure risks are identified and addressed.

7.8.4. The Students' Union give individuals specific information about the processing including the logic involved in the decision making.

7.8.5. The Students' Union shall take adequate steps to prevent errors, bias and discrimination.

7.8.6. The Students' Union shall give individuals the right to challenge and request a review of the decision.

## **8. Governance and Accountability**

8.1. The GDPR requires the Students' Union to have comprehensive but proportionate governance measures to minimise the risk of breaches and uphold the protection of personal data. The Students' Union will maintain the following streams of work that will be monitored by the Union Development Committee:

- a) Have an active data protection policy and procedures that are effectively communicated to all staff.
- b) All staff to receive basic and role specific training on data protection.
- c) Maintain relevant and up-to-date documentation on data processing.
- d) Carry out regular data protection audits across the organisation.
- e) Include data protection within the Union's risk register.

## **9. Data Security**

9.1. The Students' Union will ensure it has appropriate security to prevent personal data being accidentally or deliberately compromised. This shall be achieved by ensuring that:

- a) All staff and volunteers that have access to data have appropriate levels of data security training.
- b) Data can only be accessed, altered, disclosed, or deleted by those who have authorised to do so.
- c) Suitable and sufficient cyber security measures are in place to protect systems and devices.
- d) The data is accurate and complete.
- e) The data remains accessible and useable and has not been accidentally lost, altered, or destroyed.

9.2 All staff and volunteers are responsible for ensuring that any personal data which they hold are kept securely in line with the [University's IT Security Policies and Procedures](#) and that such data is not disclosed to any unauthorised third party.

9.3 All personal data should be accessible only to those who need to use it. A judgement on security measures shall be based on the risks presented by the data's value, sensitivity, or confidentiality. Consideration should always be given to keeping personal data: -

- a) In a lockable room with controlled access;
- b) In a locked draw or filing cabinet;
- c) If computerised, password protected.

9.4 Shared folders, files and documents shall have a clear structure and permission set to ensure that all staff or volunteers only have access to the personal information they require.

9.5 All data stored or transported on removable devices (such as memory sticks, external hard drives, mobile devices, etc.) should have an appropriate level of encryption to prevent a data breach if it is lost or stolen.

## **10. Data Transfers**

- 10.1. The Students' Union will aim to ensure all processing of data takes place within the European Economic Area (EEA).
- 10.2. Where this is not the case and personal data is shared with an organisation outside the EEA the Students' Union will seek to ensure that such organisations are based in countries that have comparable levels of personal data protection regulations to those enacted in the EEA.
- 10.3. The Students' Union will follow data transfer guidance outlined in the GDPR and from the ICO to comply with the relevant legislation.

## **11. Data Breaches**

- 11.1. The Students' Union will follow the GDPR and guidance from the ICO following any suspected or actual data breaches.

- 11.2. Any notifiable breach will be reported to the ICO, Charity Commission and the University within 72 hours after becoming aware of it.
- 11.3. All data breaches shall be appropriately investigated following and recorded.
- 11.4. The Students' Union shall have a clear response and recovery process for data breaches or cyber-attacks.
- 11.5. Should any employee, volunteer, contractor or other is found to have broken this policy or have been negligent with Students' Union data then disciplinary actions outlined in the Constitution and associated policies may be taken following an investigation.

## **12. Complaints**

- 12.1. The Students' Union will follow its complaints procedure when investigating complaints relating to data protection.