DATA PROTECTION POLICY

Policy Control:

Policy Version Number	002
Changes since previous version	• Updated formatting • Updated Job Titles • Added Mailchimp to data sharer list • Removal of first person references in request for information. • Staff Responsibilities added to Data Retention Schedule • Added line for retention of Membership events and tickets
Date Passed By Trustee Board	October 2023
Date For Review	October 2026
Policy Owner	CEO

1. Introduction and Definitions

1.1. Data Protection and GDPR is in place to protect individual's data. University of Brighton Students' Union (the 'Union' or 'BSU') take this very seriously.

1.2. In the course of carrying out its various functions and activities, the Union collects information from individuals and external organisations and generates a wide range of data which is recorded and maintained. The purpose of this policy is to enable the Union to:

1.2.1. Demonstrate its commitment to the proper handling of personal data;
1.2.2. Comply with Data Protection law;
1.2.3. Protect the organisation from the consequences of any breach of its statutory and common law responsibilities; and
1.2.4. To encourage and support a culture of best practice within data protection.

1.3. The Union is a data controller under the provisions of the Data Protection Act (ICO registration number: Z6641279). Personal data is held in compliance with the Data Protection Act (DPA) 1998 and the General Data Protection Regulation (GDPR) post 25 May 2018 and its successors.

1.4. 'Personal data' refers to information that identifies a living individual. The Union holds personal data for the following purposes:

1.4.1. **Staff Administration** – Appointments, pay, discipline, pension, work management or other personnel matters.
1.4.2. **Communication, Insights, Advertising and Marketing** – Communicating, producing insights on, advertising or marketing Union activities and services, goods and promoting public relations.
1.4.3. **Accounts and Records** – Keeping accounts, deciding to accept a person as a customer or supplier, keeping records of purchases, sales or other transactions, the processing of orders and accounts.
1.4.4. **Administration of Membership Activity and Events** – Keeping records of societies, groups and volunteer activities
1.4.5. **Advice Service and Casework** – Keeping records of advice and representation provided, and general trend analysis
1.4.6. **Fundraising** – fundraising in support of the objectives of the organisation.

1.5. The Union processes personal information about its members in accordance with the principles of the General Data Protection Regulation (GDPR) detailed below:

1.5.1. Fairly and lawfully and in a transparent manner;
1.5.2. Processed for limited purposes;
1.5.3. Adequate, relevant and not excessive;
1.5.4. Accurate and up to date;
1.5.5. Not kept for longer than is necessary;

1.5.6. Processed in line with your rights;
1.5.7. Secure; and
1.5.8. Not transferred to other countries without adequate protection

1.6. Complaints can lead to enforcement action being taken so it is vital that the Union has a workable and robust data protection policy that is understood and practiced across all sections of the organisation.

1.7. If a Chief Executive is not in post, then all actions or queries relating to that post should be addressed to the Chair of the Trustee Board.

2. Responsibilities

Staff

2.1. The Chief Executive is responsible for the general development, promotion and adherence to this policy, and ultimate responsibility for compliance by all staff.

2.2. The General Data Protection Regulation (GDPR) does not specify periods for retention.

2.3. Managers have assigned data deletion responsibilities for their areas, as defined in Appendix 1.

2.4. All staff who process personal data are expected to understand and adhere to the Data Protection Principles set out in GDPR and to ensure that they dispose of and/or destroy, confidentially where necessary, those records that have reached the end of their retention period.

2.5. The Chief Executive is responsible for ensuring that adequate and appropriate knowledge of the GDPR and the Union's legal obligation is available across the organisation. This is achieved by making available this policy and procedures, making training available to relevant groups, making new staff aware through their contracts of employment and working with the Union senior leadership team to raise relevant data protection issues for discussion, resolution and to communicate lessons learnt across the organisation.

Students

2.6. Students should assist the Union in ensuring that their own personal data as provided to the Union is accurate and up to date. Reasonable opportunities to do so will be provided.

2.7. Students volunteering for the Union may need to process personal data for activity administration purposes. If students are using personal data they must inform the relevant department manager in charge of the student's activity so that the requirements of the GDPR 2018 can be adhered to.

3. Data Collection within the Union

Staff

3.1. Staff consent to the Union using their data when they commence employment. The data collected includes personal, banking, health, disciplinary and equal opportunities information. A staff member should inform HR of any changes to information that have previously been provided, for example, changes of address or new information relevant to employment.

3.2. A confidential reference may be given to a third party for the purposes of:

3.2.1. The education, training or employment, or prospective education, training or employment, of the data subject;

3.2.2. The appointment, or prospective employment of the data subject to any office; or

3.2.3. The provision, or prospective provision, by the data subject of any service.

3.3. It will remain confidential, and is exempt from the subject access provisions, in that the subject cannot gain access from the person providing the reference. References should be marked confidential and must be approved by HR.

3.4. References may be accessible to the data subject if received from a third party. A reference could become accessible from the person to whom it is sent. Care will be taken to ensure that any reference given by the Union is founded on fact and that viewpoints expressed can be justified.

Students and Service Users

3.5. The Union Advice Service has a confidentiality policy, and users consent to the Union contacting third parties when they sign a formof authority. Personal data will only ever be processed in accordance with these consents.

3.6. Other Union departments hold information in relation to its members in order to contact students with information which may be of value to them. Members have the option to opt out of the Union but by joining give their consent to such information being collected. Information is also collected via our website for those joining student groups.

3.7. In most cases the Union will refrain from processing data relating to sensitive personal information as these matters have the potential to be used in a discriminatory way. This includes details relating to an individuals' ethnicity, religion, political opinions, health conditions, sexuality, criminal records etc. Where this is unavoidable, e.g. in the case of health and safety records, access will be limited to specific members of staff only. In circumstances where this information is required for the data processing purpose, access will be limited to specific members of staff only. Data subjects will also be required to give informed consent to the Union to use their sensitive information.

4. Data Security and Disposal

4.1. In order to prevent unauthorised processing, or accidental loss, damage or destruction, records that hold personal data are stored in locked filing cabinets, and access to IT drives, applications and servers is managed by password only.

4.2. Data is retained and disposed of according to need and in conjunction with the Data Retention Schedule (Appendix 1). At the end of the retention period data are disposed of and/or destroyed, confidentially where necessary. Manual files are shredded and electronic data is deleted from central systems.

4.3. A third party 'Memberships Solutions Limited ('MSL') will provide an information management system to store and manage our students' personal information. MSL are bound by a contract stating that personal information will not be modified, deleted, or shared, without the instructions of the Union, or used for any purpose other than that specified by the Union. They are also contractually obliged to abide by the General Data Protection Regulation. The system provider is subject to change; any future provider will be added to this policy.

5. Sharing Data

5.1. Data is shared across business functions and between staff of the Union only when it is required in order for them to perform their work function. Data is shared with external agencies, such as local authorities, the police upon request, and other organisations for volunteer and work placements. As far as possible data is transmitted solely over the secure network and the transmission of data via paper, post or independent electronic devices is strongly discouraged. The Union uses the University of Brighton network which is a secure system with fully managed access control, back-up and recovery processes in place.

5.2. The Union has no responsibility for the management of personal data processed by University of Brighton, which is solely responsible for its own compliance with the Act and GDPR. University of Brighton provides a separate notification to the Information Commissioner and is responsible for responding to requests for access to information in its possession.

5.3. The Union reserves the right to share information with the University of Brighton as necessary to pursue its legitimate interests, or to ensure the smooth operation of procedures and practices in the interests of students, staff and other individuals connected to the Union. Disclosure of personal data is always made in accordance with the GDPR and never prejudices an individual's rights or freedoms.

5.4. Under circumstances relating to disciplinary activity both the Union and the University of Brighton reserve the right to pass necessary information to the other in order to uphold and enforce disciplinary procedures.

5.5. The Union sometimes transfers data to third parties to store, manage or process students' personal information. Whenever the Union uses a third party processor, we will have a written contract in place stating that the third party must only act on the documented instructions of the Union. They are also contractually obliged to abide by the General Data Protection Regulation. The following identified parties are examples and not an exhaustive list of data processors that the Union uses:

5.5.1. Membership Solutions Limited (MSL)
5.5.2. Qualtrics
5.5.3. Advice Pro
5.5.4. Breathe HR
5.5.5. Staff Savvy
5.5.6. Mailchimp

5.6. Disclosure of personal data is always made in accordance with the principles of the General Data Protection Regulation 2018 and never prejudice an individual's rights or freedoms.

5.7. In the case of personal information requests by the police or a similar third party for the purposes of the prevention or detection of crime or for taxation, and where it is not appropriate for the requestor to seek that information from the individual(s) concerned, it may be deemed necessary to release personal data to the third party. The General Data Protection Regulation allows for a data controller (the Union) to release personal data for the purpose of:

5.7.1. The prevention or detection of crime;
5.7.2. The apprehension or prosecution of an offender; or
5.7.3. The assessment or collection of any tax or duty or of any imposition of a similar nature.

5.8. Unless a Court order is made, the decision regarding whether to release personal data will belong to the Union.

6. Request for Information, erasure and modification

6.1. In order to fulfil their responsibilities under the act, BSU will seek proof of the requestor's identity and any further information required to locate the personal data requested.

6.2. Individuals have the right to request what personal information is held about them on computer and can get access to most paper records. The General Data Protection Regulation gives individuals, as a ''Data Subject'' the right, of access to receive details of all personal information which concerns them and which is stored and processed by the Union. Request for such information should be made by the individual completing the Subject Access Request Form (Appendix 2) and forwarding it to the Chief Executive. It should be accompanied by a copy of the individual's identity document (such as passport, driver's license or University ID Card).

6.3. The General Data Protection Regulation requires the Union to provide the individual with their information within 30 days.

6.4. On occasion, the Union will process personal information to improve offers and services to enhance the student experience. This may involve profiling or automated decision making based on student information or information passed from the University. If an individual would like to object to their personal information being processed to improve the Union offers and services, they can contact the Chief Executive. There may be a legal basis to continue processing the data in this way, but each individual is entitled to an explanation of the processing and the opportunity to challenge them.

6.5. If an individual would like any of their personal information held by the Union to be blocked, erased, or destroyed, they should contact the Chief Executive.

6.6. In some cases (e.g. records relating to a criminal investigation), there may be legitimate reasons for the Union to preserve personal information. Once legitimate purposes are no longer valid, the Union will endeavour to honour any legitimate request.

6.7. Some personal information held by the Union is obtained from the University and so individuals would be required to work with the University Registry Department to remove any personal information held on University systems. On such occasions students should contact the University's Data Compliance Officer.

6.8. As a Students' Union, the Union is not a "public authority" in the sense of the Freedom of Information (FoI) Act. This means that records of the Union itself will not be covered by Freedom of Information, and cannot be requested under FoI. It is also unlikely that the Union would be considered to be covered by the Environmental Information Regulations (the definition of a "public authority" in the Regulations is broader and vaguer than that in the Freedom of Information Act).

6.9. Records which the University holds about the Union, including communications with the Union and information provided to the University by the Union, are covered by the Freedom of Information Act and the Environmental Information Regulations, and can be requested from the University.

7. Marketing and Communications

7.1. When registering with the University, students can consent for some personal details to be passed to the Union for administrative and communication purposes. Unless students have opted out, occasionally throughout their time at the University, the Union will communicate with students via email. This will be for the main purpose of communicating offers or services provided solely by the Union in line with the students' membership.

7.2. The Union is a charity, and one income stream is through marketing student appropriate offers and services provided by 3rd parties. This is done through the Union's trading company, BSU Enterprises Ltd. The Union send marketing material on behalf of its trading company where permission has been given. The Union do not sell or share personal details to third parties for the purposes of marketing.

7.3. If students would like to be removed from a mailing list they may opt out of that type of communication using the unsubscribe link provided in the email. Communications will not contain information that would not be reasonably expected given the relationship between student and the Union.

8. Data Breach

8.1. According to the General Data Protection Regulation, appropriate security of personal data is required, including protection against unlawful processing and against accidental loss or damage. To ensure this, electronic information is stored on servers managed and controlled by the Union or securely maintained on external servers by partners bound by data protection contracts. In the unlikely event of a data breach, staff have been trained to inform the Data Protection Officer who will carry out the necessary procedures.

9. Complaints

9.1. Individuals concerned about any aspect of the management of personal data at the Union are able to raise their concerns in a fair and equal way. Complaints can be registered with the Chief Executive using the Union's Complaints Policy.

9.2. If an individual feels they are being denied access to personal information they are entitled to, or feel that their information has not been handled according to the eight principles, they can contact the Information Commissioners Office:

The Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Tel: 01625 545700

Website: www.informationcommissioner.gov.uk

APPENDIX 1

Data Retention Schedule

The staff members responsible must ensure that all electronic records are deleted and any hard copies shredded in accordance with the below information.

Description of data	Retention Period	Reason for Retention Period	Staff Responsibility
Staff application forms and interview notes for unsuccessful applicants	13 months from the date of interviews	Limitation period for litigation	HR Manager
Personnel files	6 years from the end of employment	Provision of references and limitation period for litigation	HR Manager
Income Tax and NI returns, correspondence with Tax Office	6 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993	Finance Manager
Wages and salary records	6 years after the end of the financial year to which the records relate	Taxes Management Act 1970	Finance Manager
Accident Forms	6 years after the end of the financial year to which the records relate *Δ	Limitation period for litigation	CEO
Employers Liability and Directors and Officers Insurance Policies	40 years after the end of the financial year to which the records relate	Limitation period for litigation	CEO
Insurance Claims and Policies (other than listed above)	6 years after the end of the financial year to which the records relateΔ	Limitation period for litigation	CEO
Membership information; society/sports/groups/ volunteers/surveys	3 years after the end of the financial year to which the records relate*	Provision for references / alumni communications / insight	Engagement Manager and Marketing & Comms Mgr (MSL)
Membership Event/Ticket Sales	3 years after the end of the financial year to which the records relate*	Provision for refund / insight	Engagement Manager and Marketing & Comms Mgr (MSL)
Suppliers	6 years after the end of the financial year to which the records relate	Limitation period for litigation	Finance Manager
Advice Casework	6 years after the end of the financial year the student leaves the University*	Provision for complaints against service, or to substantiate actions taken against another service	Support Manager
Commercial Event/Ticket/Outlet Sales	6 months after the event has taken place*	Provision for potential complaints / refunds	Director of Commercial Services and Marketing & Comms Mgr (MSL)
Emails (other than HR)	12 months after the end of the financial year to which the records relate**	Provision for reference	All staff

*Anonymised demographic data may be retained for comparison and reporting

**HR Emails will be retained for 6 years in accordance with all other Personnel File

Δ Unless a longer retention period is required due to specific legislation (eg relating to asbestos or radiation)

APPENDIX 2

Brighton Students' Union Subject Access Request Form

To the Chief Executive,

I,_____wish to have access to data which the University of Brighton Students' Union has about me in the following categories:

(Please tick as appropriate)

- ☐ Personnel File / Application
- ☐ Advice Case Notes
- ☐ Membership Activity information (eg. Societies, Events Attendance, Course Representatives)
- ☐ Health and Safety Records
- ☐ Finance Accounts and Records
- ☐ Personal details held including name, address, date of birth etc
- ☐ Other information: please list below

……

The speed of search would be assisted if you are willing to providing details of relevant date ranges or any specific incident/activity that your request is relating. This is not a requirement of your request.

……

……

Full Name: …… Date: ……

Signed: ……

I have attached a copy of the following ID to confirm my identity:

……

Please read the Union's Data Protection Policy for the full information regarding Subject Access Requests.

Union Admin Section

Date Received: Received By:

Request Outcome: