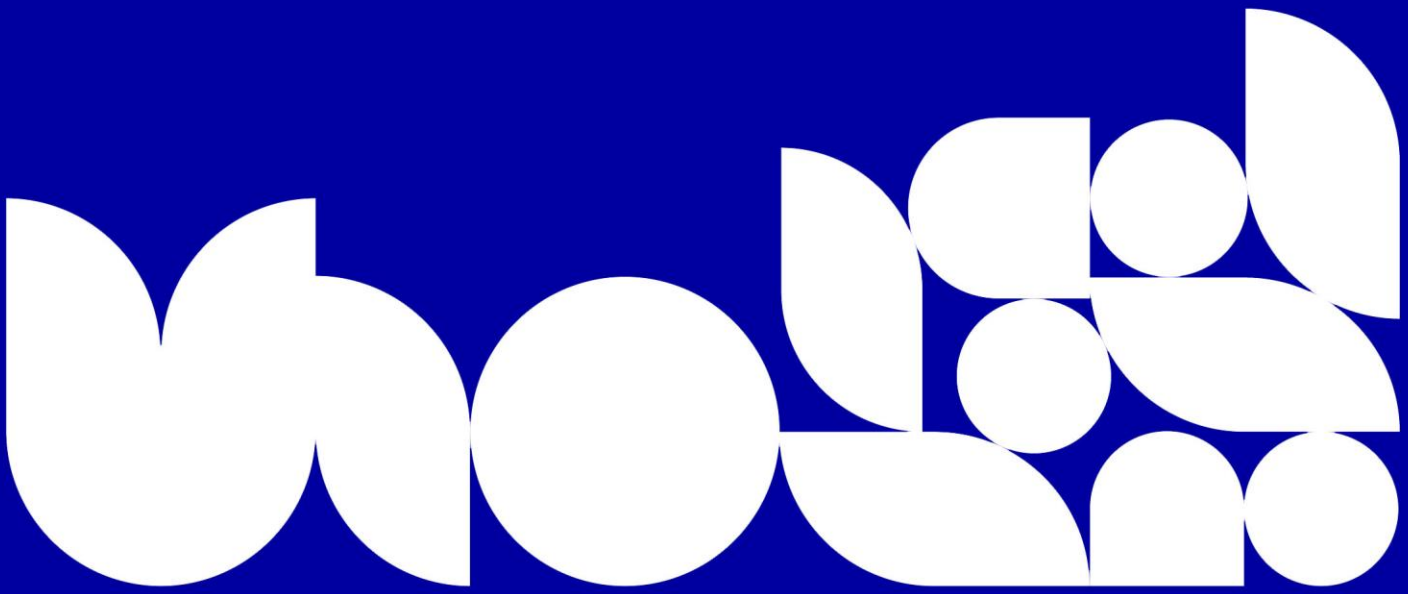
THE SU BATH



The SU Data Policy

1. Students' Union/University relationship

1.1 The SU recognises that its responsibility for data protection is shared with the University of Bath because:

- they are the employer of all SU staff;
- they provide The SU with its IT systems and equipment;
- they are the University at which The SU student members are registered at.

1.2 The SU recognises that this relationship could cause confusion. Therefore The SU will ensure in setting out the following policy and any relating procedures that these are in line with the University's own where reasonably appropriate.

2. Policy statement

2.1 The SU recognises that data protection is an integral part of good management.

2.2 The SU aims to meet our data protection commitments by:

- ensuring data protection concerns and breaches are taken seriously, investigated and acted on as appropriate;
- ensuring SU staff, student leaders and volunteers are familiar with this policy and receive training on their responsibilities;
- reporting to the Information Commissioner's Office *(ICO)* any serious data breaches that pose a likely risk to people's rights and freedoms;
- reporting to the Charity Commission if a serious incident happens or is suspected to have taken place.

3. Responsibilities for data protection

3.1 The University of Bath are responsible for:

- ensuring appropriately secure IT systems are in place and maintaining them;
- providing advice and guidance on data protection matters.

3.2 The Board of Trustees are responsible for:

- setting and monitoring strategy and policy;
- monitoring data protection performance and seeking reassurance that performance is satisfactory;
- reporting to the Charity Commission if a serious incident happens or is suspected to have taken place in relation to The SU.

3.3 The Director for Student Leadership and Support is responsible for:

- ensuring the data policy is put into practice;
- recommending to and monitoring improvements for the Board of Trustees where data protection performance is found to be unsatisfactory;
- reporting to the Information Commissioner's Office (ICO) and Board of Trustees any serious data breaches that pose a likely risk to people's rights and freedoms;
- annually reviewing the data sharing agreement in place with the University.

3.4 The Data, Research & Insight Manager is responsible for:

- liaising with the University on data protection matters and ensuring this policy is up to date;
- the design and implementation of local data protection procedures as they apply to The SU;
- monitoring data protection performance across The SU and providing assurance reports to the Board of Trustees;
- managing an ongoing programme of audits of compliance with The SU data protection policy on behalf of the Board of Trustees.

3.5 The Website and Digital Manager and Data, Research & Insight Manager are responsible for:

- liaising with the University for the transfer of student data to The SU;
- ensuring that student, and other, data is maintained securely within the Customer Relationship Management System (MSL);
- advising Heads of Departments and managers on compliance and good data practice.

3.6 Heads of Departments and managers are responsible for:

- having an appropriate awareness of the data policy and the requirements of legislation as they apply to the work of their department/team;
- ensuring that staff (including contracted staff), student leaders and volunteers are made aware of and understand the data policy along with any related procedures;
- ensuring that staff, student leaders and volunteers complete any necessary data protection training relevant to their area of work.

3.7 All staff, student leaders and volunteers are responsible for:

- completing any mandatory data protection training required for their role;
- co-operating with supervisors and managers on data protection matters;
- ensuring any data they handle is done so in accordance with this policy;

- reporting all data protection concerns and breaches to an appropriate person *(as detailed within this policy)*.

4. When this policy applies

4.1 This policy applies to any personal data which is collected and/or handled by The SU or any of its Student Groups.

4.2 Personal data is any data *(physical or digital)* which identifies an individual *(directly or indirectly)* and provides information relating to them.

4.3 Staff, Student Leaders and volunteers are all responsible within The SU for ensuring that any personal data they collect and/or handle is done so in accordance with this policy.

5. How The SU uses personal data

5.1 The SU uses personal data where it is relevant and there is a legitimate need, including for the following purposes:

- to identify and represent the views of Student Members;
- to provide services, products or information asked for;
- to administer membership, including membership of SU Groups e.g. clubs, societies and networks;
- to set-up voting permissions for SU elections and referendums;
- to contact members about formal matters that we are required to by law;
- to enable us to respond to queries/requests efficiently and accurately;
- to understand how we can improve our services, products or information;
- to tailor marketing and communications to individual preferences;
- to provide an efficient and smooth website experience;
- to uphold other SU policies;
- to ensure The SU is compliant with regulatory practices and processes.

5.2 The SU will occasionally send Student Members information about products and services it thinks will be of interest to them during their time at the University of Bath.

5.3 Student Members who have agreed to receive marketing communications may always opt out at a later date by unsubscribing or updating their preferences on their website profile page.

6. Collecting personal data

6.1 When students complete registration at the University of Bath they automatically become members of The SU. This includes agreeing to a statement that relevant personal data will be shared with The SU[1].

6.2 As part of a Data Sharing Agreement the University shares personal data with The SU on the basis that there is a legitimate interest for students to be offered with the membership services provided by the Union, which include representation functions. [See Appendix A for further detail]

6.3 As part of a data sharing agreement the University shares as standard the following personal data with The SU:

- Student ID;
- Title, first name, middle name, surname, preferred name, gender, and date of birth;
- University email address, mobile phone number and home address;
- Faculty, department, course name, course code, course end date and year of study;
- Type of Student: Undergraduate, Postgraduate taught, Doctoral;
- Fee status: Home, EU, Overseas student;
- Mode of study;
- On placement;
- Nationality and country of residence;
- SAMIS student status *(Current student, suspended etc)*;
- Additional data fields are by agreement where there is a legitimate need and are listed in Appendix A, this can include special category data.

6.4 Personal data must only be collected where necessary and only used for the purpose it was originally intended for.

6.5 This should normally be in accordance with a purpose already set out in The SU Data policy.

6.6 Where personal data needs to be collected for a purpose not covered by the Data policy then the:

- purpose for collecting the personal data must be declared at the point of collection;

[1] Data Protection Statement for student registration

- recorded consent of the individual(s) the personal data relates to must be secured and kept.

6.7 Under no circumstances should personal data be:

- indirectly collected about an individual without their consent *(such as from their social media account)*;
- auto-populated or added to by the person collecting the personal data.

6.8 The SU collects and processes the following personal data about service users related to SU activity:

- Group memberships, committee roles, representative roles and other voluntary roles;
- Photography & filming taken at events;
- Award nominations, event plan submissions and vehicle hires;
- Insurance claims;
- Records of ticket/product purchases/refunds;
- Bank details to facilitate payments;
- Records of training completed through The SU;
- Disability disclosure forms;
- Event/trip details including dietary requirements or access needs;
- Advice & support student case files.

6.9 This personal data is shared directly by service users with The SU on the basis of consent and that there is a legitimate interest for this to be provided in order to deliver the services they are using.

7. Special category data

7.1 The SU will not collect the following data unless there is a legitimate need as agreed in advance by the Chief Executive, a record of all agreements will be maintained:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data *(where used for identification purposes)*;
- data concerning health;
- data concerning a person's sex life; and

- data concerning a person's sexual orientation.

7.2 Under GDPR this data is classified as special category data and additional appropriate controls will be required if such data needs to be collected or used.

8. Storing personal data

8.1 The SU has agreements in place with third parties to store and/or process data securely on our behalf. A full list of current third parties is documented in Appendix B.

8.2 With the exception of the above, personal data will not be shared by The SU with any other third parties *(except where required by law)* without the permission of the individual to whom the data relates to.

8.3 Each of the organisations listed above have their own privacy policies which can be found on their websites.

8.4 Personal data must only be kept as long as necessary to achieve the purpose it was originally collected for.

8.5 The SU keeps:

- student records and membership details for six years after they leave the University before being disposed of automatically by MSL or deleted manually where downloads or local records have been kept;
- student member disciplinary records and complaints for four years following graduation/leaving the University before being disposed of manually by staff;
- student advice and support case notes are automatically deleted by AdvicePro after a case has not been active for more than 6 years;
- Outlook emails, Teams messages and Forms are deleted in line with Microsoft's deletion schedule;
- student reimbursement records for seven years before being disposed of by the Finance Team.

8.6 Under no circumstances should personal data be kept and stored on:

- non-work computers and/or other personal non-work electronic devices;
- portable storage devices *(i.e. USB keys)*;
- non-work personal email accounts.

8.7 To ensure security, personal data collected must only be kept and stored in:

- a restricted confidential folder located on the X drive;
- a restricted shared platform accessed through the Microsoft 365 Suite;
- a record on the restricted access platform AdvicePro;
- a restricted folder located in a locked cabinet in a secure SU office;
- a restricted section of MSL *(The SU Customer Relationship Management System)*.

9. Sharing personal data

9.1 Personal data must never be shared with anyone *(third party)* outside The SU unless:

- required and permitted to do so by law *(such as for the prevention of crime)*;
- a data sharing agreement is in place with the third party;
- a contract is in place with the third party permitting them to process the personal data;
- recorded consent has been given for it by the individual*(s)* that the personal data relates to.

9.2 If uncertain contact the Data, Research & Insight Manager or Senior Administrator (Governance) for further advice.

10. Cookies

10.1 Cookies are small text files stored on your device when you visit a website. They help websites work properly and provide useful information to improve your experience.

10.2 Types of cookies we use:

- Essential cookies: These are strictly necessary for the website to function (e.g., login, shopping cart). They do not require consent.
- Functional cookies: These enhance your experience (e.g., remembering preferences). Consent is required.
- Analytics cookies: These help us understand how visitors use our site by collecting anonymised data. Consent is required.
- Third-party cookies: Some pages may include cookies from advertisers or partners for analytics or advertising purposes. These require consent.

10.3 Your consent:

By law, we must ask for your consent before placing non-essential cookies on your device. You will see a pop-up banner where you can choose to accept, reject, or manage your cookie preferences. You can change your choices at any time. More

information related to cookies used by The SU can be found at https://www.thesubath.com/privacy/website/cookies/

10.4 Managing cookies:

You can remove or block cookies through your browser settings. For detailed instructions, visit https://www.aboutcookies.org/how-to-manage-and-delete-cookies

11. Subject Access Request

11.1 Under GDPR individuals have the following rights in relation to their personal data:

- right of access - the right to ask for copies of your personal information;
- right to rectification - the right to ask for personal information you think is inaccurate or incomplete to be rectified;
- right to erasure - the right to ask for your personal information to be erased in certain circumstances;
- right to restriction of processing - the right to ask for the processing of your personal information to be restricted in certain circumstances;
- right to object to processing - the right to object to the processing of your personal information in certain circumstances;
- right to data portability - the right to ask that personal information you gave The SU be transferred to another organisation, or to you, in certain circumstances;

11.2 To exercise any of the rights above an individual should email su-cda@bath.ac.uk.

11.3 The requester should provide the following in the email:

- provide a scanned copy of their ID card for verification purposes;
- indicate from a list provided what personal data they want to be provided with;
- indicate a timeframe they want us to carry out this request for;
- indicate which data subject rights they wish to exercise.

11.4 A request will be actioned within one month of confirmation of the subject access request being received. If longer than a month is required to fulfil a request the individual must be informed of the reason.

11.5 Where an individual chooses to view, access or be provided with a copy of their personal data The SU may be required to redact personal data belonging to third parties *(students, members of public or other organisations)*.

11.6 If personal data is to be provided to an individual it will be password protected and this will be given at a meeting *(in person or online)* so as to visually confirm that the individual matches the ID card.

11.7 The SU will keep a record of the request, any information given and emails exchanged with the requester.

12. Data Breach

12.1 The Senior Administrator (Governance), Data, Research & Insight Manager, Director of Student Leadership & Support and/or Chief Executive should be informed immediately if:

- personal data has gone missing and cannot be found;
- personal data has been shared with an unauthorised third party;
- personal data has been stolen by a third party.

12.2 In the event of a data breach the individual*(s)* to whom the personal data relates to will be informed:

- of the likely consequences of the personal data breach;
- of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects;
- the name and contact details of a contact point within The SU where more information can be obtained.

12.3 If a data breach poses a likely risk to people's rights and freedoms the Information Commissioners Office (ICO) must be notified within 72 hours of becoming aware of it.

12.4 If this happens The SU must provide the ICO with:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- the name and contact details of a contact point within The SU where more information can be obtained;
- a description of the likely consequences of the personal data breach;

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

12.5 If the ICO must be informed of a data breach this will also be fully reported to the Board of Trustees.

13. Making a complaint

13.1 If an individual has any concerns about The SU's use of personal information, they can make a complaint to The SU in accordance with the complaint's policy by emailing su-cda@bath.ac.uk.

13.2 They can also complain to the ICO if they are unhappy with how The SU has used their data.
Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.
Telephone number: 0303 123 1113
Website: https://www.ico.org.uk

Reviewed 12/2025

Next Review 12/2026