THE STUDENTS' UNION *(THE SU)* DATA PROTECTION POLICY

Rationale: To set out how The SU adheres to the General Data Protection Regulation *(GDPR)*

Students' Union/University relationship

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.

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.

Policy statement

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

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.

Responsibilities for data protection

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.

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.

Reviewed:	03/2022
Next Review:	03/2024

The Chief Executive is responsible for:

- ensuring the data protection 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.

The Governance & Executive Support Manager and Website Manager are 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.

Heads of Departments and managers are responsible for:

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

All staff, student leaders and volunteers are responsible for:

- 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)*.

When this policy applies

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

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

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.

Collecting personal data

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

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

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

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

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

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.

Special category data

Under no circumstances should the following data be collected without the Chief Executive's explicit permission:

- 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.

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

Storing personal data

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

- a restricted confidential folder located on the X drive;
- a restricted folder located on 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)*.

To request a restricted folder on the X drive please contact the Governance & Executive Support Manager.

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.

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

Sharing personal data

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 *(see Privacy policy)*;
- a contract is in place with the third party permitting them to process the personal data *(see Privacy policy)*;
- recorded consent has been given for it by the individual*(s)* that the personal data relates to.

If uncertain contact the Governance & Executive Support Manager for further advice.

Reviewed:	03/2022
Next Review:	03/2024

Subject access request

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;

To exercise any of the rights above an individual should complete an online subject access request form.

The online form will ask the requester to:

- 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.

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

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)*.

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.

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

Data breach

The Governance & Executive Support Manager 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.

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.

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.

If this happens The SU must provide the ICO with:

- a description of the nature of the personal data breach including, where possible:

Reviewed:	03/2022
Next Review:	03/2024

  - 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.

In the event that the ICO must be informed of a data breach this will also be fully reported to the Board of Trustees.

ICO Data protection fee

Every organisation or sole trader who processes personal information needs to pay a data protection fee to the ICO, unless exempt. The SU is exempt from paying this fee because it is a not-for-profit organisation.

A not-for-profit organisation can make a profit for its own purposes *(charitable or social)* but the profit should not be used to enrich others. Any money raised should be used for the organisation's own activities.

In order to qualify for this exemption The SU must:

- only process information necessary to establish or maintain membership or support;
- only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;
- only hold and/or process information about individuals whose data is needed for this exempt purpose.

Reviewed:	03/2022
Next Review:	03/2024