



Data Protection Policies and Procedures:

1. Principles:

- 1.1 The Union understands and places great importance on the 1998 Data Protection Act and the General Data Protection Regulations. This document alongside the Unions privacy statement and data storage policy outlines how the Union complies with both pieces of legalisation.
- 1.2 This policy refers to both electronic and physical data the Union controls and processes. For more information on the safeguards the Union has in place for each type of data please refer to the Data Storage Policy.
- 1.3 In this statement, "website" means Beds SU at www.bedssu.co.uk.
- 1.4 Beds SU permits access to your data with ARRK (<http://www.arrkgroup.com>), as a data processor as our website provider, for the sole purpose of technical support and for no other purpose or use.
- 1.5 Beds SU shares anonymous student trend and lifestyle habits with the National Union of Students (NUS) (<http://www.nus.org.uk>) for the purpose of obtaining national trends and representational themes.
- 1.6 Beds SU permits access to your data with Fidelity Systems as a data processor (<http://www.fidelitysystems.co.uk>) for the purpose of technical support of our EPOS and instant loyalty system and for no other purpose or use.
- 1.7 Beds SU permits access to your data with Advice Pro as a data processor (<https://secure.advicepro.org.uk>) for technical support of our advice service software and for no other purpose or use. Advice Pro shares social Policy themes captured on Advice Pro in an anonymous manner with the National Union of Students.
- 1.8 We use SJ Creatives (<http://www.sj-creative.co.uk>) for graphic and digital asset design where data shared will be restricted to photos of unnamed individuals and direct quotes provided from students and service users and for no other purpose or use.
- 1.9 We use QBC Agency (<http://www.qbcagency.co.uk>) for graphic and digital asset design where data shared will be restricted to photos of unnamed individuals and direct quotes provided from students and service users and for no other purpose or use.

- 1.10 Beds SU may use other organisations, such as mailing houses, as a data processor in order to deliver a service or communication message to you. In the event of this, the Union will enter into a data processing agreement with such organisations, on the terms that data can only be used to administer the project specified and that all data will be destroyed following the project specified.
- 1.11 If you are a University of Bedfordshire student, we will communicate to you via email by virtue of you opting into this during the University enrolment process. You can express your desire not to receive such emails through your online account settings, which you can change at any point in time.
- 1.12 If you are a guest, we will only communicate to you via email when you express your desire to do so through your online account settings, which you can change at any point in time.
- 1.13 Every Beds SU staff member has a clear data protection statement included in their contract of employment with the Union and in addition will receive online data protection training on commencement of their employment within the organisation alongside a separate introduction meeting with the Unions data protection officer outlining our policies and procedures to ensure compliance.
- 1.14 Student Committee Members that have access to your data will do so on the provision of them agreeing to a clear data protection agreement.
- 1.15 Student Committee Members will only have access to data for groups that they have been elected to manage.

2. Data We Hold:

2.2 Data from the University of Bedfordshire will be automatically and electronically loaded into the website database in line with the data sharing agreement Beds SU holds with the University of Bedfordshire. In addition to the data received from the University of Bedfordshire, we record your online behaviour such as purchase history.

2.3 If you are not a student at the University of Bedfordshire we simply hold the data you provide during the website registration process and records of your online behaviour such as purchase history.

2.4 We do not hold any bank account/ credit card details (except those of our staff members for the purposes of payroll and expense payments) and do not hold University passwords, as student 'log ins' are processed through a single sign on process administered by the University of Bedfordshire.

2.5 We may from time to time collect additional data via online forms and will only use the data collected from these forms to administer the activity or service we are requesting the information for.

3. Where is Data Held:

3.1 Data that is received from the University of Bedfordshire and through online behaviour recording is stored in Amazon's (AWS) European Data Centre in the Republic of Ireland.

3.2 Data received from online forms used on the website is held on a secure server based in the United Kingdom and provided by My 1&1 Internet Limited (<https://www.1and1.co.uk>).

3.3 EPOS and loyalty account details are stored in a secure server operated and administered in conjunction with the University of Bedfordshire's Information Communication Technology department.

3.4 Data related to advice casework is held on a secure server operated and administered by Advice Pro and is located within the United Kingdom.

4. Why Do We Hold Data:

4.1 We hold data; to ensure we can offer you an interactive website experience, to ensure only students and student groups can access certain parts of the website, to ensure we can conduct equal opportunities monitoring, to ensure you a hassle-free e-commerce experience and communicate information relevant to you. For more information refer to our [privacy policy](#)

5. Data Security:

5.1 The importance of security for all personally identifiable information associated with our users is of utmost concern to us. We take technical, contractual, administrative and physical steps to protect all of the user information we hold. Despite this, you acknowledge and accept that no system can be guaranteed to be 100% secure.

5.2 It is important for you to protect against unauthorised access to your password and to your computer. Be sure to log out when using a shared computer and take steps to make sure your personal information has not been stored by that computer or a network connected to it.

6. Cookies:

6.1 Cookies are very small text files that are stored on your computer when you visit some websites. We use cookies to help identify your computer so we can tailor your user experience, track shopping basket contents and remember where you are in the order process. You can disable any cookies already stored on your computer, but these may stop our website from functioning properly.

6.2 For more information on the cookies we operate please visit our online disclaimer at www.bedssu.co.uk/disclaimer and our privacy statement at www.bedssu.co.uk/privacy.

7. Your Responsibilities:

2.1 You are responsible for; keeping your device free from viruses, your personal data safe and the protection of your username and password.

2.2 Further responsibilities and conditions are outlined in our online disclaimer at www.bedssu.co.uk/disclaimer

8. Request for Information Held:

8.1 Should you wish to request the information the website holds upon you, please do so in writing to su.data@beds.ac.uk. Information will be provided for reasonable requests upon the satisfactory obtaining of identification.

9. Breach Management:

9.1 The Union will respond to a suspected data breach or breach through the following step by step process:

- Any breach or suspected breach will be immediately secured to prevent data leak or further data leak.
- An investigation will be undertaken by the Data Protection Champion and the University will be informed and consideration will be taken as to whether the breach is reportable to the Information Commissioners Office (ICO).
- Any individual affected by the breach will be contacted and any action they can/should take will be explained to them.
- Recommendations will be made to the Senior Management Team and Trustee board on how such an occurrence can be avoided in the future.

10. Tracking Records:

10.1 The Union will produce a regularly updated recording and tracking portal which will record:

- Actions in relation to compliance with the Unions retention of data
- Logs of data transfer from the University to the Union
- Information on new data processing activities
- Actions undertaken requested by an individual
- Analysis of website registrations

11. Areas of Responsibility:

11.1 The table below outlines areas of responsibilities for each of the different areas of main data capturing and processing the Union undertakes.

Area:	Data:	Responsibility:	Accessible To:	Safeguarding:
Website database	As described in the privacy policy	Head of Marketing and Communications	Beds SU Staff based on modular access to only relevant areas	<p>Online data protection training.</p> <p>Data protection agreement / data storage policy</p> <p>Specific website training upon induction</p>
Online forms	Collected for a specific purpose such as market research	Head of Marketing and Communications	Senior Management and Relevant Staff Members	Survey and form collection policy and operational procedures that includes template statements and clear guidance of anonymising data after analysis.
Student Groups	Membership details and emergency contact details	Head of Membership Services	Committee Members	<p>Student group data protection policy and procedures.</p> <p>Specific training and briefing to all student group leaders to ensure compliance.</p> <p>Specific data protection agreements before access are granted.</p>
Advice Service	Case notes and demographic	Head of Membership Services	Advice Service Staff	<p>Informed consent process before data is captured.</p> <p>Advice service standards and procedures.</p>

				Specific training and CPD.
Democracy	Voting records and candidate information	Head of Membership Services	Senior Management and Relevant Staff Members	Online data protection training Data protection agreement and data storage policy Specific website training upon induction.
Finance	Financial records, statements, staff expenses and bank account details	Head of Finance and Resources.	Finance and HR Staff	Held in a secure environment Financial procedures and processes Specific training upon induction.
Human Resources	Application details and HR records	Head of Finance and Resources.	Senior Management and Finance and HR Staff	Application consent process Explicit consent upon induction from staff Online data protection training. Data protection agreement, and data storage policy
Marketing	Communication preferences	Head of Marketing and Communications	Senior Management and Relevant Staff Members	Digital opt in and out solution.
EPOS and Loyalty	Name and student ID Number.	Head of Marketing and Communications	Senior Management and Relevant Staff Members	Online data protection training Data protection agreement and data storage policy

				Specific EPOS training upon induction.
Staff email accounts	Emails which may include personal information.	All employees with an email account	All employees with an email account	Email use policy. Automatic deletion set on email accounts.

Policy Number:	Approving Body:	Date Ratified by Board:	Renewal Date:
3.V2	Senior Leadership Team	October 2018	October 2020

