Data Protection Policy
Appendix
Guidance to Staff

The following document will outline the responsibility of those employed by Beds SU, in relation Data Protection and ensuring the organisations is compliant with the General Data Protection Regulations Act 2018.

Understanding Data Protection.

The General Data Protection Regulation Act 2018 (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).

GDPR provide legislation under 7 key principles:

1. **Lawfulness, fairness and transparency** - Personal data must be processed lawfully, fairly and in a transparent manner.
2. **Purpose limitation** - Personal data can only be collected for a specified, explicit and legitimate purposes.
3. **Data minimisation** - Data collection must be adequate and limited to what is necessary for the collected and stated purpose of processing.
4. **Accuracy** - Personal data must be accurate and where necessary kept up to date.
5. **Storage limitation**- Personal data should not be kept for longer than is necessary to undertake the specified data processing task.
6. **Integrity and confidentiality (security**) - Personal data should be processed in a manner that ensures appropriate security and protection of the data.
7. **Accountability** – Where personal data is collected it is the responsibly of the organisation and its employee to ensure this is compliant under the legislation

Responsibilities of Beds SU Employees

1. All employees must be aware of and adhere to the Information Commissioners Office guidelines on data protection, the Data Protection Act 1998 and the General Data Protection Regulations.
2. All employees must only hold personal sensitive data in accordance with the notice given to the information commissioner's office which can be found online at https://ico.org.uk/ESDWebPages/Entry/Z8045836
3. All employees must operate in accordance with the data protection agreement with the University of Bedfordshire.
4. All employees must adhere to the Unions; privacy policy and data protection policy and should make the Senior Management Team aware if items are missing from the policy from activities relating to data protection are undertaken within their roles**.**
5. All employees must undertake Data Protection Training as required
6. All employees must be aware of and adhere to the Unions data retention periods and participate in regular audits and data impact assessments.

7. All employee are to ensure adequate security measure are in place to protect any personal data they hold
8. Employees should only be collecting and processing data for a legitimate and specified purposed as outlined in the Unions charitable objectives or as required by the Charities Act, Education Act or other relevant legalisation.
9. Under no circumstances is data to be shared with any other organisation, other than those clearly outlined in our Data Protection Policy. (authorities such as the police are exempt)
10. Under no circumstances is data to be collected for direct marketing purposes. All direct mail is to be sent via the Beds SU website.

Union Data Protection Policies
All Beds SU Staff should read and ensure they understand the Unions Policies in relation to Data Protection. These can be found at www.bedssu.co.uk/dataprotection

Staff Developments & Training
Staff required to collect and/or handle personal data must complete the following before doing so:

1. Read the Beds SU Data Protection policies found at www.bedssu.co.uk/dataprotection
2. Complete and pass an online Data Protection course which can be provided to you by the Data Protection Champion.
3. Attend a presentation provided by the Data Protection Champion that outlines Beds SU key policies and procedures.
4. Complete a declaration form, confirming you have received adequate training and understand and will adhere by the Union Data Protection policies and procedure.

Furthermore, staff will be required to attend additional training deemed required at any time.

Sending Emails
All staff are required to ensure the following email signature is included on all emails sent on behalf of Beds SU. It will provide recipient with important data protection information.

[Forename Surname]
[Title]

[telephone number] | [Location] | www.bedssu.co.uk

Data Storage & Security

It is adviced that staff take particular note of the Unions data security procedures (Data Protection Policy Appendix: Security Procedures) to ensure that clearly understand the protocols in place to maintain the safe storage and management of personal data

Employee Computer/Digital device protection

The following measure must be taken by employees to protect data stored on their allocated computer device:

1. All employees are bound by the University of Bedfordshire's computing regulations and policies which include the safe use of strong passwords and correct and safe use of computing equipment.
2. All employee with computer equipment must ensure these are password protected and take adequate measure to ensure their computer is locked when they are not in attendance of it.
3. Staff must all ensure that adequate virus protection has been installed and correctly set up on their computer (support available from the Data Protection Officer or university ICT team)

Data Collection activities

Additional consent is needed to for any collection of data outside that specified in the Data Protection policy. In this instance student must be informed of the following and give their explicit permission to the use of their data.

1. Why you are collecting the data and how it will be processed
2. Where the data will be held
3. The legal basis for collecting the data
4. How long the data will be held for

5. A link to www.bedssu.co.uk/dataprotection to inform them of their rights, how to complain and the Unions policies

Data Collection Privacy Notice Template
The following are examples of a typical privacy notice's that might be used for the purpose of personal data collection via information forms, surveys, competitions. Please note that these templates are to act as guidance only as they may not cover all aspects required for a specific task. If in doubt, contact the Data Protection Champion (su.data@beds.ac.uk).

1. **Information Forms** (e.g, dietary requirements form, participation form, preferences form, nominations form etc) -

   I understand and agree that by completing this [name of form] I am giving the Union explicit permission to use my details for the purpose of [what are you using the data for] only and for no other purpose. I understand that the Union will hold this information until [date that the data will be deleted, or the incident that would trigger its deletion]. This is to ensure that [reason for needing the data for the length of time required]. I understand that I can access information on what data the Union holds, how it is managed, my rights and how to make a complaint through referring to the Union privacy policy online at www.bedssu.co.uk/dataprotection

2. **Surveys and Questionnaire** (e.g, GOATs, Feedback, Union Research etc)

   'I understand and agree that by completing this [survey/feedback form/questionnaire] I am giving the Union explicit permission to use my views in reports and statistical publications in relation to the questions asked. I understand that the views I give in this [survey/feedback form/questionnaire] will only be used for generating a report on the topic being asked and the Union we will only publish demographic data in which I will not be able to be personally identified. I further understand that I can remain anonymous by not providing my Student ID. I understand the Union will use my student ID to draw demographic data on myself from the Union's online database for analysis but once completed my student ID will be deleted and thus responses will not be able to be linked back to myself. Finally, I understand that I can access information on what data the Union holds, how it is managed, my rights and how to make a complaint through referring to the Union privacy policy online at www.bedssu.co.uk/dataprotection

3. **Competitions** (please note a competition may also form part of a privacy notice for a Survey or information form. This would be to be incorporated into one of the above privacy notice templates:

   I understand and agree that by completing this [Competition name] I am giving the Union explicit permission to use my details for the purpose of [what are you using the data for] only and for no other purpose. I understand that the Union will hold this information until the after the competition has closed and following communication with the winner. This is to ensure that a winner can be chosen and informed via [how will the winner be contacted]. I understand that I can access information on what data the Union holds, how it is managed, my rights and how to make a complaint through referring to the Union privacy policy online at www.bedssu.co.uk/dataprotection

Seeking support and further Guidance

If staff require to undertake any of the following actions, they should seek advice from the Data Protection Champion before conducting the activity.

1. Collecting new types of data
2. Using new software
3. Storing data in a new way
4. Undertaking automated decision making or profiling
5. Sharing data with a third party

Reporting a suspected data protection breach

Data Breach - This refers to “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”

There can be three types of breech:

1. Confidentiality breach
2. Availability breach
3. Integrity breach

Example of a Breach include (this is not an exhaustive list) –

1. Loss or theft of hard copy notes, USB drives, computers or mobile devices.
2. An unauthorised person gaining access to your laptop, email account or computer network.
3. Sending an email with personal data to the wrong person.
4. Not adhering to procedures in place that protect the rights of the individual.

You must report suspected breach to the Data Protection Lead or member of the Senior Leadership Team as soon as you become aware, ensuring:

1. reporting take priority before any other work-related task;
2. steps within your ability to minimise and further impact of the breach;
3. steps have been taken to notify third party technical suppliers where possible.

The Data Protection Champion will investigate and take steps to ensure further security of the data if required. The Data Protection Champion will make recommendation to the CEO to whether the suspected breach must be reported to the ICO.

Data Protection Champion

Any questions or concerns regarding should be directed to the union allocated Data Protection Champion, Lisa Roerig.