Data Protection Policy

Policy Contents:

1. Definition of data protection terms

1.1. The following provides a brief explanation of the key terms used within the Data Protection Act 2018, and which are helpful to understand when consulting this document:

1.1.1. Data protection - the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data.

1.1.2. Data - information in a form which can be processed. It includes both automated data and manual data. Automated data means any information on computer or information recorded with the intention that it is processed by computer. Manual data means information that is kept/recorded as part of a

relevant filing system or with the intention that it should form part of a relevant filing system.

1.1.3. Personal data - data relating to a living individual who is or can be identified either from the data or, from the data in conjunction with other information.

1.1.4. Sensitive personal data - relates to specific categories of data which are defined as data relating to a person's:

- racial or ethnic origin
- political opinions or religious or philosophical beliefs
- physical or mental health or condition
- sexual life
- criminal convictions or the alleged commission of an offence, any proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings
- trade union membership

1.1.5. Data Subject - A data subject is a living individual to whom data relates to.

1.1.6. Data Controllers - those who, either alone or with others, control the contents and use of personal data.

1.1.7. Data Processor – those who processes personal information on behalf of a data controller

1.1.8. Data processing - Data processing means performing any operation or set of operations on data, including: (i) obtaining, recording or keeping data; (ii) collecting, organising, storing, altering or adapting the data; (iii) retrieving, consulting or using the data, disclosing the information or data by transmitting, disseminating or otherwise making it available; (iv) aligning, combining, blocking, erasing or destroying the data.

2. Policy Statement

2.1. Every individual (a data subject) has rights with regard to how their own personal data and sensitive personal data is collected and handled. A data subject also has the right to know what data we have on them and request access to it at any time. During the course of our activities we will collect, store and process the personal information of individuals. It is incumbent upon us to treat their data responsibly, with respect to their rights and applicable law.

2.2. We process personal information in accordance with the principles of the Data Protection Act 2018; we will ensure personal information is:

2.2.1. processed lawfully, fairly and in a transparent manner in relation to individuals;

2.2.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (further processing for archiving purposes in public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes);

2.2.3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

2.2.4. accurate and, where necessary, kept up to date (every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay);

2.2.5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals); and,

2.2.6. processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.3. This policy and related documentation demonstrate Beds SU compliance with the data protection principles and its responsibilities as a data controller and, on occasion, data processor.

2.4. All employees and volunteers who process personal data are expected to understand and adhere to this policy.

2.5. Beds SU will meet its responsibilities under this policy by making available this policy and procedures to all colleagues; by regularly reviewing practices and systems engaged in the processing of personal data, in accordance with this policy; via compulsory training and development for employees and volunteers; and through ongoing training and development for colleagues with access to sensitive data, and with management responsibility.

2.6. This policy applies to all personal data (including sensitive personal data) processed by Beds SU. The types of information that we may be required to handle include details of current, past and prospective students, employees, suppliers, customers, organisational networks (such as the University of Bedfordshire, National Union of Students and other students' unions) and others that we communicate with.

2.7. The Data Protection Lead shall be the Chief Executive Officer, which may be delegated; and Beds SU shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

3.1. All data processed by Beds SU is to be done on one of the following lawful basis: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).

3.2. Beds SU shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

3.3. Beds SU will use, when appropriate and proportionate, Data Protection Impact Assessments (DPIA)*[It need to build this and ad to appendix]* to ensure that the collection and use of data falls within the law and is for the legitimate needs of the organisation.

3.4. Privacy Notices will outline the lawful bases for processing personal data and provide sufficient, but not overbearing detail on why data is collected and retained and how it is used by the charity, stored and disposed of. Individuals will also be informed of their rights.

3.5. Beds SU shall take reasonable steps to ensure personal data is accurate.

3.6. To ensure its processing of data is lawful, fair and transparent, Beds SU will document its processing activities and review this periodically by auditing the data processed across its activities. The audit of the data processed by Beds SU shall outline the purposes of processing, the categories of individuals it processes data for (e.g. employees, members, suppliers, etc.) and categories of personal data it processes.

3.7. The CEO is responsible for ensuring that adequate and appropriate knowledge and competence for good data protection exists across the organisation; this may be delegated. The Senior Leadership Team are responsible for the oversight of relevant data protection issues and should raise these for discussion, resolution and communication across Beds SU.

4. Data Archiving and Removal

4.1. Legislation does not specify periods for the retention of all personal data processed. Beds SU will consider the Data Protection Principles, business needs, legitimate interests and any professional and legal guidelines, in determining how long it stores specific types of data.

4.2. To ensure that personal data is kept for no longer than necessary, Beds SU shall put in place a Data Retention Schedule, which identifies what data should/must be retained, for how long, and why.

4.3. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Union systems.

4.4. Data is retained and disposed of according to need and in conjunction with the Data Retention Schedule. At the end of the retention period Beds SU will dispose of, or destroy all data, confidentially where necessary; we shred paper files and delete electronic data from central systems.

5. Data Sharing

5.1. Beds SU will share data across different business functions, and colleagues only when it is required in order to perform necessary work.

5.2. Significant data sharing occurs between Beds SU and the University of Bedfordshire, which supports the legitimate, necessary functioning of Beds SU and its charitable mission. For example, the University of Bedfordshire provides data of all students in order for Beds SU to maintain a register of Members that, among other things, supports the meeting of regulatory requirements.

5.3. We sometimes share data with external partners, such as the University of Bedfordshire and the National Union of Students, under specific Data Sharing Agreements. We also utilise common online platforms under agreement with third parties, for example Microsoft, that support the necessary functioning of the business.

5.4. Due to the close partnership between Beds SU and University of Bedfordshire, which is necessary for the strategic functioning of the charity and is governed by a Memorandum of Understanding, some organisational systems used to process personal data are managed by the University of Bedfordshire. Beds SU uses a secure network system to retrieve, manage and hold student data provided via a data sharing agreement with the University of Bedfordshire.

5.5. Beds SU also uses a secure network system with fully managed access control, back-up and recovery processes in place. These systems are identified in this policy 'Data Sharing' appendix.

5.6. As far as possible data is transmitted solely over a secure network connection, and the transmission of printed data through the post, or through independent electronic devices, is strongly discouraged.

6. Security

6.1. Beds SU will ensure that personal data is stored securely using sophisticated software that is kept up-to-date as reasonably as possible. Personal data stored on paper records are to be used only in reasonable, necessary circumstances.

6.2. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- "Confidentiality" means that only people who are authorised to use the data can access it.
- "Integrity" means that personal data should be accurate and suitable for the purpose for which it is processed.
- "Availability" means that authorised users should be able to access the data if they need it for authorised purposes.

6.3 In order to prevent unauthorised processing, or accidental loss, damage or destruction, paper records that hold personal data are stored in locked filing cabinets, and electronic records are stored in drives, applications and servers that are securely managed.

6.4 Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

6.5 When personal data is deleted this should be done safely such that the data is irrecoverable.

6.6 Appropriate back-up and disaster recovery solutions shall be in place.

6.7 Appropriate measures will be taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

7. Data Breach

7.1. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Beds SU shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

7.2. Beds SU will maintain and make available to employees, and upon reasonable request, a protocol for dealing with breaches of this policy.

7.3. A Data Breach Report will be maintained that sensitively detail occurrences of data breaches.

8. Data Subject Requests

8.1. Individuals have the right to access their personal data and any such requests made to Beds SU via su.data@beds.ac.uk shall be dealt with in a timely manner.

8.2. Beds SU will provide a set protocol to managing and responding to Data Subject Access Requests.

8.3. Whilst Beds SU welcomes requests to access data that it holds, it will need to authenticate the identity of any individual who makes a Subject Access Request. Beds SU may also need to ask for more information before it can process the request and locate the data.

8.4. There may be limitations on information the SU provides as part of requests; in these cases, the SU shall provide a reasonable explanation in reference to ICO guidance.

8.5. Procedures for the charity's Advice Service, or other sensitive aspects of data processing in the SU, may have further limitations or alternative safeguards for the protection of data, organisational risk and privacy, and as such these procedures will

take precedence over contradictions in this policy, save for any oversight from the Data Protection Lead.

9. Complaints

9.1. Any person who is concerned about any aspect of the management of personal data can contact the Data Protection Champion in writing to su.data@beds.ac.uk

9.2. Any person who feels they are being denied access to personal information they are entitled to, or feels that their information has not been handled according to the Data Protection Principles, can contact the Information Commissioners Office at any time at 'The Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.' The Information Commissioner's website is www.ico.org.uk and their telephone number is (+44) 1625 545700.

Policy Number:	Approving Body:	Date Ratified by Board:	Renewal Date
3.V3	Senior Leadership Team		