Data Storage Policy

Beds SU is committed to storing data and files in an accessible, secure and managed manner. This policy provides an outline and guidance surrounding:

- The Union preference is to store files and data electronically
- Guidelines for the storing of electronic data and files
- Guidelines for the storing of non-electronic data and files
- Guidelines surrounding the holding of personal sensitive data

1. **Beds SU data/files storing preference:**

    a. The Union has the preference of all data and files being stored electronically due to its value of sustainability and the level of security, accessibility and backup capability of stored electronically stored files.

    b. If an employee recognises a need to store files/data in a non-electronic manner a request should be made to the relevant Senior Leadership Team (SLT) member for approval.

2. **Guidelines for the storing of electronic data and files:**

    a. All departmental files relating to the running of the activities within the department should be stored in the relevant Office 365 SharePoint group.

    b. All email activity should be set to automatically delete after a two year calendar period (730 days).

    c. All confidential files should be stored in individual One Drive folders which can be shared appropriately with other members of staff as deemed appropriate.

    d. All engagement data, personal sensitive data and student record data must be stored in one of the following applications; UnionCloud, Machform, Fidelity, HR Online, Business Safe, Advice Pro, Bright HR, Staff Savvy, Survey Monkey (market research only) or Tableau.

    e. Employees are not permitted to store information/files on; local C drives, memory sticks, Dropbox or any other location unless permission is obtained from the relevant Senior Leadership Team (SLT) member.

f. Storing data on servers outside of the EU is strictly prohibited without permission from the CEO and staff must undertake checks when using software and services.

g. All employees should undertake an annual audit of any data/files stored and only hold data that is still relevant and useful for the organisation and is legally compliant. This audit should be completed using the audit toolkit provided.

h. 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.

i. Any loss of electronic equipment must be reported to the relevant Senior Leadership Team (SLT) member immediately.

j. All employees are prohibited from allowing non Beds SU employees to use the encrypted electronic equipment.

k. Any security breaches must be reported to the relevant Senior Leadership Team (SLT) member immediately.

3. Guidelines for the storing of non-electronic data and files:

a. If permission is obtained from the relevant Senior Leadership Team (SLT) to store data/files in a non-electronic format the employee must ensure the data/files are stored in a secure location only accessible to relevant individuals.

b. The employee must only store the information for as long as legally required or until the information is required for them to undertake their daily duties.

c. Once the files/data are no longer required the employee must arrange for the confidential recycling of such data/files.

d. Although the organisation promotes using electronic equipment for meetings staff are permitted to print papers for meetings but once the employee has attended the meeting they must arrange for the confidential recycling of printed materials.

e. Any handwritten notes should be stored in a safe and secure manner and confidentially recycled once they are no longer required by the employee.

4. Guidelines surrounding the holding of personal and sensitive data:

a. 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.

b. 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

c. All employees must operate in accordance with the data protection agreement with the University of Bedfordshire.

d. All employees must adhere to the Unions; privacy policy and data protection policy always 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.

e. All employees must undertake the online data protection training and have a data introduction meeting with the data protection officer before any access to data is provided.

f. All employees must be aware of and adhere to the Unions retention policy of data which can be found in the Unions data protection policy.

g. All departments must produce a data risk assessment that is reviewed annually and a Data Impact Assessment (DIA) when using new technologies or new processes involving data. Any DIA needs the approval of the Senior Leadership team at a leadership meeting.

h. All holders of MacBook's must ensure their devices are encrypted and that the passwords used to access them following the Universities password policy.

i. 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.

j. Employees may only share data with a third-party service provider once a signed data processing agreement has been agreed and signed by the CEO and this must only be done on the basis that that data can only be used to administer the project specified and that all data will be destroyed following the project specified.

k. The above point will not apply to the Unions Advice Service sharing data with individuals involved in representational cases. The Advice service will obtain explicit consent from students before sharing data with third parties. The student will be informed when giving explicit consent.

5. General Data Protection Regulations:

a. All employees and student leaders (with access to data) will be given a briefing and training on the General Data Protection Regulations through the following responsibilities and means:

i. Career Staff (CEO Responsibility) – Annual staff briefing session, online induction training and induction meeting with the Data Protection Officer and signed bespoke data protection agreement.

ii. Student Leaders (Head of Membership Services Responsibility) – Inclusion in committee training, bespoke data protection agreement and briefing on the Student Groups Data Protection Policy.

iii. Student Staff (Relevant Line Manager) – inclusion in induction training and bespoke data protection agreement. Depending on the nature of the role and level of data certain student staff members will, in addition, be required to undertake online training and have an induction meeting with the Data Protection Officer.

b. All employees and student leaders should make themselves aware and following the following procedures in relation to the rights of individuals under the General Data Protection Regulations:

i. **The right to be informed** – When collecting data from any means other than the Universities data feed or using the data for a purpose not stated within the privy policy the employee/student leader working with their relevant Senior Manager must ensure the full information required is provided to a data subject in a clear and easily understandable format and that the individual gives informed and explicit consent before collecting any data alongside a mechanism to withdraw such consent at any point.

ii. **The right of access** – If an employee/student leader receives an access request this should be passed onto the Data Protection Officer.

iii. **The right to rectification** – If an employee/student leader receives a rectification request this should be passed onto the Data Protection Officer.

iv. **The right to erasure** – If an employee/student leader receives an erasure request this should be passed onto the Data Protection Officer.

v. **The right to restrict processing** – If an employee/student leader receives a restricting process request this should be passed onto the Data Protection Officer.

vi. **The right to data portability** – All employees/student leaders collecting data must ensure that if it is requested it can be done so in an open source format such as CSV.

vii. **The right to object** – If an employee/student leader receives an objection request this should be passed onto the Data Protection Officer.

Rights in relation to automated decision making and profiling – If an employee/student leader is planning on implementing automated decision making and profiling activity that must plan this alongside the Data Protection Officer to ensure the correct safeguards and notices are in place.

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