Data Protection Policy
Appendix
Security Procedures

This document set outs the organisations practices and processes in order to ensure the security of both electronic and non-electronic data held by the Union.

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.

Main Organisational Network

As the Union uses the main University network to ensure data security our employees and volunteers will be bound by and follow any non-conflicting elements of the following University policies and procedures when using the University network to ensure data security and promote best practice;

1. Anti-Virus policy
2. Bring your own device policy
3. Data Security Policy
4. Interception Policy
5. Network Acceptable Use Policy
6. Network Password Policy
7. Software Licencing Policy
8. Use of mobile telecommunications

In addition to the above, the Union actively works with the Universities ICT team ensure the ongoing enhancement and implementation of data security.

Third Party Software and Cloud Storage and Servers:

Before contracting, engaging with or using any third-party software, cloud storage and servers the Union will undertake due diligence and gain appropriate assurances that;

i. The provider is able to demonstrate is compliant with the General Data Protection Regulations (GDPR).
ii. Where further reassurances are required and its deemed appropriate, the Union may enter into a Data Sharing agreement with a third party, which will be approved and sign by the CEO and relevant person from the third party.

Internal Protocols for enhancing Data Security

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. 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.

Storing of electronic data and files:

1. All departmental files relating to the running of the activities within the department should be stored in the relevant Office 365 SharePoint group.
2. All confidential files should be stored in individual One Drive folders which can be shared appropriately with other members of staff as deemed appropriate.
3. 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.
4. 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.
5. 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.
6. Any loss of electronic equipment must be reported to the relevant Senior Leadership Team (SLT) member immediately.
7. All employees are prohibited from allowing non Beds SU employees to use the encrypted electronic equipment.
8. Any security breaches must be reported to the relevant Senior Leadership Team (SLT) member immediately.

Storing of non-electronic data and files:

1. 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.
2. 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.
3. Once the files/data are no longer required the employee must arrange for the confidential recycling of such data/files.
4. 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.
5. Any handwritten notes should be stored in a safe and secure manner and confidentially recycled once they are no longer required by the employee

Security protection of Union Computers/digital devices

It is important for you to protect against unauthorised access Union computer equipment and other electronic devices. All Beds SU 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.

All Beds SU computer devices are to be password protected and have adequate virus protection software installed and correctly setup.

Other Computers/digital devices

Where in exceptional circumstances Beds SU employee maybe required to use personal computers and digital devices, this will require agreement from their line management. In this instances employee will be required to ensure the Union data protection policy and procedures continue to be adhered to.