Data Breach Reporting Policy

1. Context:

a) This policy exists to give employees, volunteers and student leaders clear guidelines of what to do in the event of a data breech or a suspected data breech. It further acts as a vehicle to ensure that data breeches are:

i. Detected as soon as possible;
ii. Dealt with through effective and efficient action;
iii. Categorised and monitored in a consistent and centralised manner;
iv. Assessed and responded to in an appropriate manner;
v. Prevented from further damage, impact and spread;
vi. Used as an opportunity to review practices and procedures;
vii. Where appropriate reported to the Information Commissioners Office;
viii. Used as a vehicle to ensure lessons are learnt.

b) This policy should be read in conjunction with the following data protection policies and procedures which are in place to ensure the Union follows the General Data Protection Regulations (GDPR) and manage data in a safe and secure manner to reduce the risk of data breech:

i. Privacy Policy;
ii. Data Protection Policy;
iii. Data storage policy
iv. Standard data protection sharing agreement;
v. Beds SU data risk assessment;
vi. Departmental data risk assessment.

2. Definitions:

a) The General Data Protection Regulations define a data breech as “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”

b) The General Data Protection Regulations further define data breeches into three further definition classifications:

i. “Confidentiality breach” - where there is an unauthorised or accidental disclosure of, or access to, personal data.

ii. Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

iii. "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

c) The table below shows common types of data breeches with would be covered under this policy and the most likely Union operations that would be subject to such data breeches:

Type:	Examples:	Departments / Services:
Technical	Data Corruption Viruses Malware Corrupt Website Code Hacking	All
Physical	Unescorted visitors in secure areas Break-ins to sites Thefts from secure sites Theft from unsecured vehicles/premises Loss in transit/post	All
Human Resources	Data Input errors Non-secure disposal of paperwork Unauthorised disclosures	HR/Finance
Human Error	Loss of data Inappropriate storage of data Insecure storage of data	All
Policy Breech	Not adhering to retention policy Not adhering to data protection policy Not adhering to privacy policy Not obtaining consent	All

3. Employee Responsibilities:

a) Each employee with ensure the following is undertaken within their department and individual working practices:

i. Strict adherence to the Unions privacy policy;
ii. Strict adherence to the Unions retention policy;
iii. Strict adherence to the Unions data protection policy;
iv. Strict adherence to the Unions data storage policy;
v. Strict adherence to this policy;
vi. Ensuring policies and procedures are adequate in own area of operation;
vii. Ensuring volunteers/student leaders have appropriate training;
viii. Ensuring safeguards are put in place for volunteers/student leaders;
ix. Ensuring reporting procedures for volunteers/student leaders;

x. Ensuring robust data sharing agreements are in place with third parties;
xi. Ensuring appropriate due diligence is undertaken with third parties;
xii. Ensuring their department has an adequate data risk assessment;
xiii. Ensuring an annual departmental data audit is undertaken.

b) During working hours, each employee will report a suspected or actual data breech as soon as they become aware of it using the online reporting tool at www.bedssu.co.uk/dbr

c) Should the online forms server or website be compromised the staff member should report the breech over email to su.data@beds.ac.uk

d) In the event that that the email system has been compromised in addition to the forms server and website the staff member should verbally report the incident to a member of the Senior Leadership Team.

e) Out of the hours each employee with complete the online reporting tool and additionally contact the on duty Senior Leadership Team member using the Unions emergency reporting procedure.

f) Each employee will further:

i. Ensure reporting is a priority before any other work-related task;
ii. Take steps within their ability to minimise the impact of the breach;
iii. Take steps to notify third party technical suppliers where possible.

4. Union Response to Potential Breeches:

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

i. Any breach or suspected breach will be immediately secured to prevent data leak or further data leak.

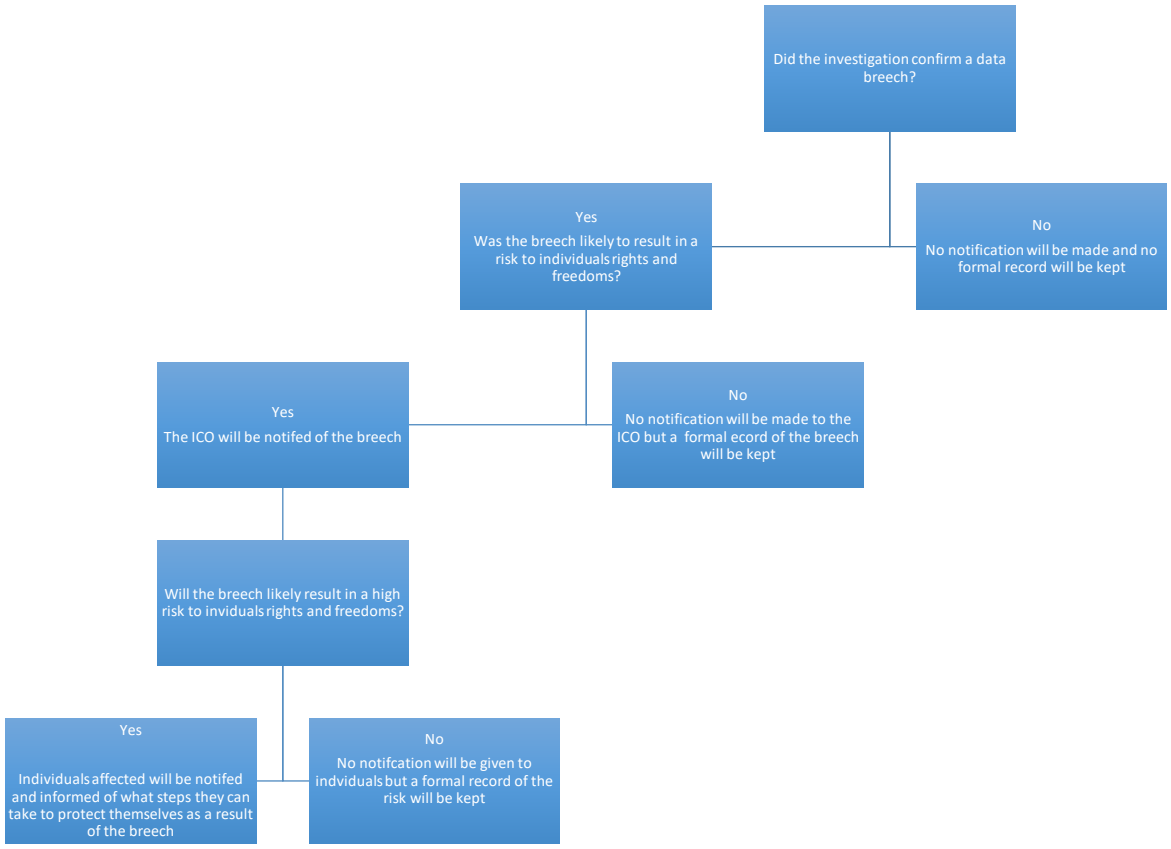
ii. An investigation will be undertaken by the Data Protection Champion and the University will be informed and consideration will be taken as to whether the breach is reportable to the Information Commissioners Office (ICO) with 72 hours.

iii. Any individual highly affected by the breach will be contacted and any action they can/should take will be explained to them.

iv. Recommendations will be made to the Senior Management Team and Trustee board on how such an occurrence can be avoided in the future.

5. Guidance on Authority and Individual Reporting:

a) The flow diagram below shows the process the Union will follow when making decisions about notifications and reporting:



b) The following guidance will be used to aid and determine the risk to rights and freedoms of individuals. However, due to the complexity of data the Union holds and different potential routes and causes of breeches each case will require individual considerations and interpretation due to the nature and importance of the data

Measure:	Low Risk	Medium Risk	High Risk
The type of breach	Data that is no longer available by corruption or accidental deletion	Data that has been lost but not suspected to have been disclosed	Data that has been disclosed to unauthorised third parties or bodies.
The nature of data	Widely available through several sources	Available but through a limited number of sources	Not readily or publically available from other sources
The sensitivity of the data	None or low personally sensitive data	Moderately personally sensitive data	High or very high personally sensitive data

The volume of data	Limited or incomplete data about an individual	Limited but complete data about an individual	More than one complete set of data about an individual
The ease of identification of individuals	Highly unlikely to be able to identify and individual	Unlikely to be able to identify and individual	Likely to be able to identify and individual
Severity of consequences for individuals	No risk of fraud, physical harm, psychological distress, humiliation or damage to reputation.	Unlikely risk of fraud, physical harm, psychological distress, humiliation or damage to reputation.	Likely risk of fraud, physical harm, psychological distress, humiliation or damage to reputation.
Special characteristics of the individual	No special characteristics (children or other vulnerable individuals) or other safeguarding considerations.	No special characteristics (children or other vulnerable individuals) but other safeguarding considerations.	Special characteristics (children or other vulnerable individuals) with/ without other safeguarding considerations.
The number of individuals affected	Less than 5 individuals involved.	5 to 100 individuals involved.	Over 100 individuals involved.
Special characteristics of the data controller	No data involved in relation to our exceptions to hold certain types of data as a not for profit.	Less sensitive data involved in relation to our exceptions to hold certain types of data as a not for profit.	Moderate or highly sensitive data involved in relation to our exceptions to hold certain types of data as a not for profit.
General consideration	Low risk to the rights and freedoms of individuals being affected	Moderate risk to the rights and freedoms of individuals being affected	High risk to the rights and freedoms of individuals being affected

6. Guidance on Record Keeping:

a) Regardless of whether or not a breach needs to be notified to the supervisory authority, the controller must keep documentation of all breaches. In order to do achieve this the Union will:

i. Discuss and minute conversations about data breeches at Senior Leadership team meetings;
ii. Report data breeches to the board of trustees along with action plans of how to minimise further risk and implement lessons learned;
iii. Document the investigation, reporting decision, SLT and board discussions and actions taken in a admin area alongside the reported breech.