Lincoln Bishop University

Lincoln Bishop University

Document Administration

Document Title:	Data Breach Policy	
Document Category:	Policy	
Version Number:	2.0	
Status:	APPROVED	
Reason for Development:	To define the Data Breach process for staff and students	
Scope:	All staff and students	
Author/Developer:	Chief Planning & Data Officer	
Owner:	Chief Planning & Data Officer	
Assessment: *(where relevant)*	Assessment Type: Equality Assessment Legal Information Governance Academic Governance	Assessment Status: COMPLETE NOT REQUIRED COMPLETE NOT REQUIRED
Consultation: *(where relevant)*	Consultation Type: Staff Trade Unions via HR Students via Students' Union Any External Statutory Bodies	Consultation Status: NOT REQUIRED NOT REQUIRED NOT REQUIRED
Authorising Board:	University Council	
Date First Authorised:	June 2017	
Reviewed & Effective From:	04 February 2025	
Next Review Due*:	June 2028 – *unless required earlier*	
Document Location:	University Website	
Document Control:	All printed versions of this document are classified as uncontrolled. A controlled version is available from the University Website.	
Alternative Format:	If you require this document in an alternative format, please contact policy@lincolnbishop.ac.uk	

Please Note: *This document remains valid until formally revoked or replaced by the University.*

DATA BREACH POLICY

VERSION CONTROL TABLE

Version Number	Date Authorised	Summary of Key Changes
1.0	June 2017	Policy first issued and approved by University Executive Group
1.2	June 2018	Housekeeping Update
2.0	04 February 2025	Full review and amendments

Lincoln Bishop University

DATA BREACH POLICY

1. INTRODUCTION

1.1. Lincoln Bishop University (LBU; The University) collects, holds, processes and retains personal data to deliver and support its business function.

1.2. Under the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018) the University has an obligation to ensure the appropriate safeguards are in place when handling personal data.

1.3. The University needs to have in place a robust and systemic process of reporting and managing any incidents involving the breach of personal data.

2. SCOPE

2.1. This University policy applies to all personal data processed by the University, regardless of format and is applicable to all staff, students, visitors, contractors and data processors acting on behalf of the University.

2.2. One of the requirements of the GDPR is that, by using appropriate technical and organisational measures, personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

2.3. Staff awareness of policy and procedures in relation to data breaches, and data protection, is essential to ensure the University is in a position to comply with the requirements of the GDPR, and the DPA.

3. UNDERSTANDING AND IDENTIFYING A DATA PROTECTION BREACH

3.1. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. This policy applies to both breach incidents that are confirmed to have taken place and suspected breaches that require appropriate University staff to investigate the incident.

3.2. It can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

3.3. Examples of data security breaches may include:

3.3.1. Loss or theft of data or equipment on which data is stored e.g. loss of laptop, USB stick or paper record
3.3.2. Unauthorised disclosure or Restricted/Confidential Data
3.3.3. Equipment theft or failure
3.3.4. Human Error
3.3.5. Hacking Attack

3.4. The GDPR only applies where there is a breach of personal data. For the purpose of this policy, not all security incidents are personal data breaches, all personal data breaches are security incidents. Any security breaches concerning personal data confirmed or suspected should follow this policy.

4. AIM

4.1. The aim of this policy is to promote and standardise the University wide approach and response to any data breach incident, to ensure incidents are reported, logged and managed appropriately by adopting a standard consistent approach to all data security incidents it aims to ensure that:

4.1.1. Incidents are reported in a timely manner and can be properly investigated.
4.1.2. Incidents can be managed by relevant stakeholders, skilled and authorised personnel, and consideration given to the referral to the Information commissioners/supervisory authority where appropriate to do so, ensuring the 72 hours statutory period is met.
4.1.3. All incidents are recorded and documented, evidence gathered and maintained in a form that will withstand internal and external scrutiny.
4.1.4. The notification of any data subjects and/or external bodies where appropriate.
4.1.5. The impact of incidents and actions taken to prevent reoccurrence and identify improvements in policies, procedures and Records Management Principles.

5. RESPONSIBILITIES

5.1. The University Executive Group (UEG) has overall responsibility to ensure that the University meets its legal and regulatory obligations and is accountable to the University Council for ensuring these obligations.

5.2. The Data Protection Officer (DPO) has responsibility to brief and escalate data breaches where necessary to the Vice-Chancellor or submission. The DPO will determine the necessity to report to the Information Commissioners Office/Supervisory authority and make recommendations.

5.3. University Leadership Group (ULG)/ Line Managers/ System Owner/System Stewards are responsible for ensuring that staff in their area are in compliance with the policy and provide appropriate assistance to investigations as required.

5.4. Information Users – All staff, contractors will be aware of their responsibilities and reporting procedures where there is a personal data breach whether actual, suspected or potential should;

5.4.1. Providing accurate information in connection with any alleged breach, to the DPO in a timely manner.

5.4.2. Being aware of the GDPR and the DPA, and what they mean for the University.

5.4.3. Being aware of the University's Data Protection Policy.

5.4.4. Attending any relevant training sessions as required including classroom training and electronic learning programmes, as directed by Human Resources.

6. REPORTING A SUSPECTED BREACH/INCIDENT

6.1. Staff and Students are required to report the breach/incident via the Data Breach via the HelpDesk or alternatively, by sending an email to informationcompliance@lincolnbishop.ac.uk.

6.2. Please see Appendix 1 for guidance on the information that should be contained within your incident report.

7. INCIDENT CONTAINMENT & RECOVERY

7.1. Once a Data Breach has been reported, the case will be reviewed first by a member of the IT Team, should immediate IT precautions or action be required to be taken.

7.2. The DPO will then review the report and will undertake the following as required in the circumstances.

7.3. Liaise with the individual who reported the potential breach to obtain as much information as possible. Liaise with System Owner(s) or and IT where necessary and convene a breach response team to carry out investigations /actions if necessary.

7.4. Take steps to contain the breach and take any immediate steps to prevent any further breach which may require input form specialist departments.

7.5. The relevant parties should be notified in a timely manner to ensure it is given the priority and action required.

7.6. Conduct assessment of severity, risk and harm to individuals.

7.7. Consider notification of relevant third parties and those individuals impacted.

7.8. Record the breach and the management plan of the breach actions and results within the Data Breach Incident Log.

7.9. Under no circumstances are staff, other than the DPO or those dutifully requested to do so, contact or engage in the investigation or communicate with the Data Subject.

8. SUGGESTED ACTIONS FOR STAFF TO TAKE TO RECOVER OR MITIGATE A BREACH

8.1. For email breaches:

8.1.1. Try to recall the message using the Outlook recall action.

8.1.2. If you are unable to recall the email, contact the IT HelpDesk to ask if they are able to recall it.

8.1.3. Send a follow-up email to the recipient to request deletion, using the following statement:

"You have been sent an email in error from my contact address. You are asked to disregard the content and delete the email immediately.

Please confirm in writing that the deletion has taken place and that the information has not been further shared or forwarded to anyone else."

8.1.4. Contact the recipient(s) directly and ask that the email is disregarded, seeking written confirmation of the above actions.

8.1.5. Update informationcompliance@lincolnbishop.ac.uk of recovery actions taken.

8.2. For other Hard Copy or Removable Media breaches:

8.2.1. Seek to retrieve the paperwork or removable media immediately.

8.2.2. Ensure it has not been accessed or shared further. If the items have been found by an individual, request confirmation from them that they have not accessed, copied or shared further. It is important you act quickly, if necessary, liaise with supervision to avoid any delay in implementing remedial action.

8.2.3. Contact informationcompliance@lincolnbishop.ac.uk for further advice and support.

9. NOTIFICATION OF BREACH

9.1. The University has a duty to report to the Information Commissioner's Office (ICO) a personal data breach that is likely to result in high risk to the Rights and freedoms of individuals within 72 hours.

9.2. If the assessment of risk and impact identifies that the breach meets the threshold for referral the DPO will liaise with the Vice-Chancellor and report the notifiable breach to the ICO/Supervisory Authority either via telephone or via the online reporting form.

10. EVALUATION & RESPONSE

10.1. Following every incident of a personal data breach it is important to investigate causes and evaluate our response to it. Existing controls will be reviewed to ensure adequacy and any changes required to policies and procedures.

10.2. To simply contain and continue business as usual is not acceptable and incidents will be reported on and follow up actions undertaken to minimize the risk of a similar incident reoccurring in the future.

10.3. Failure to comply or remedy the required actions requested by the DPO, which are required to mitigate potential repeat breaches, will lead to disciplinary action, and in some cases may be considered as acts of gross misconduct.

11. CONCLUSION

11.1. Any member of staff or student who suspects a data breach has occurred, or who is made aware (from a source outside of the University) of an alleged breach/incident, must report it immediately.

12. APPENDIX 1 – DATA BREACH INCIDENT REPORTING

Data Breach is reported via the HelpDesk using the 'Data Breach' button.

1. Information to be included in the declaration:
   - 1.1 Date & Time of Breach/Incident
   - 1.2 Faculty/Department
   - 1.3 Description of Breach/Incident and how it occurred
   - 1.4 If a Data Breach has occurred, was any protected characteristic data included in the breach? (please refer to Guidance Note 1)
   - 1.5 How many subjects have been affected, and who? (please refer to Guidance Note 2)
   - 1.6 Number of personal data records concerned (if applicable)
   - 1.7 Describe and identify any potential risks and impact to the affected data subject(s) given the sensitivity of the data and any other risks identified
   - 1.8 What actions have already been taken to recover the breach or mitigate the risk
   - 1.9 Have the data subjects been made aware? If so, when and by whom?
   - 1.10 Type(s) of Breach (Please refer to Guidance Note 3)
   - 1.11 Person Completing this form:

Guidance Notes

Note 1 – Protected Characteristics

Age, Race, Disability, Sex (Gender), Sexual Orientation, Religion or Belief, Transgender, Pregnancy and Maternity, Marriage and Civil Partnership.

Note 2 – Data Subject Categories

Employees, Students, Children, Vulnerable Adults, Research Participants.

Note 3 – Types of Breach

The University classifies the breaches into different types depending on the incident. Please see Notes 4 to 8 for further information.

Note 4 – Data Loss

Any loss of data including missing discs, USB memory sticks, paper files, etc.

Note 5 – Inappropriate Disclosure

Includes the accidental or deliberate sharing of information to the incorrect person/ organisation, wrong emails or information provided about the wrong data subject.

Note 6 – Unauthorised Access (incl. Cyber Incident)

The accessing or attempts to gain unauthorised access to data (both via computer, verbal or hard copy) that is not for a legitimate purpose. Changes to a systems hardware or software without the Systems Owner's consent or malicious disruption.

Note 7 – Procedural Concerns

This is where a breach occurs however we have followed the current procedure, and it is identified that the procedure may require review.

Note 8 – Data Theft

Theft of laptops, discs, mobile phones, briefcases that contain information

13. APPENDIX 2 – ABBREVIATIONS & GLOSSARY

the University or LBU	Lincoln Bishop University.
ICO	The Information Commissioner's Office (ICO) is the regulatory authority in the United Kingdom in relation to data compliance, regulation and oversight.
GDPR	The EU General Data Protection Regulation
DPA	The Data Protection Act (2018). This constitutes the UK law on data protection and exists alongside the EU GDPR
Data Protection Officer/DPO	The member of University staff responsible for Data Protection
Data Controller	A Data Controller determines the purposes and means of processing personal data. The University acts as the Data Controller for data it collects
Data Processor	A Data Processor is responsible for processing personal data on behalf of a Data Controller. The University may process data for external organisations. The University may also engage third party organisations (Data Processors) to provide services on its behalf
Personal Data	Any information relating to an identifiable natural person who can be directly or indirectly identified in particular by reference to an identifier. The GDPR applies to 'Personal Data', meaning any information relating to an identifiable natural person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal Data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute to a particular individual

DATA BREACH POLICY

Data Subject	A natural person whose personal data is processed by a controller or processor
Data Processing or Processing	Everything the controller does with personal data, throughout the record life-cycle. Processing encompasses each activity from the collection of personal data through to its deletion or destruction. Processing therefore includes, but is not limited to, the storage, updating, sharing, editing, copying, printing and maintenance of the data
Data Breach	A breach of security leading to the accidental or unlawful access or disclosure of personal data transmitted, stored or otherwise processed in connection with the needs of University business
Sensitive Personal Data/Special Categories of Personal Data	GDPR refers to sensitive personal data as “Special Categories of Personal data” (see Article 9). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individuals. Personal data relating to Criminal Convictions and Offences are not included, but similar extra safeguards apply to its processing (see Article 10 of the GDPR)