BISHOP GROSSETESTE UNIVERSITY

Document Administration

Document Title:	Data Breach Policy
Document Category:	Policy
Version Number:	1.2
Status:	Approved
Reason for development:	Update and review
Scope:	This procedure applies to staff, students, and relevant data subjects
Author / developer:	Head of Quality and Regulatory Compliance
Owner	University Secretary / Chief Operating Officer
Assessment: (where relevant)	Tick relevant assessments Tick if not applicable ☒ Equality Assessment (mandatory) ☐ Legal ☐ ☒ Information Governance ☐ ☐ Academic Governance ☐
Consultation: (where relevant)	☐ Staff Trade Unions via HR ☐ Students via Bishop Grosseteste University Students' Union ☐ Any relevant external statutory bodies
Authorised by (Board):	Senate
Date Authorised:	26 March 2018
Effective from:	March 2018
Review due:	March 2021
Document location:	University Website
Document dissemination / communications plan	Emailed to key staff, the Students' Union, Student Advice, the University website. The policy shall be well publicised and made easily available to students and employees of Bishop Grosseteste University or anyone on the University's behalf whose duties involve data privacy and security protection or who collects, accesses, maintains, distributes, processes, protects, stores, uses, transmits, disposes of, or otherwise handles personally identifiable information.

Document control:	All printed versions of this document are classified as uncontrolled. A controlled version is available from the University website.

1. Purpose

1.1. The purpose of the policy is to:

- establish the goals and the vision for the personal data breach response process.
- clearly define to whom it applies and under what circumstances,
- to define a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritisation of the incidents),
- set out reporting, remediation, and feedback mechanisms.

1.2. Bishop Grosseteste University (BGU) intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches. The policy outlines how BGU’s established culture of openness, trust and integrity should respond to such activity. BGU is committed to protecting BGU's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

2. Definition

2.1. For the purpose of this policy a personal data breach is defined as:
“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”

3. Scope

This policy applies to all students and employees of BGU. It covers any subject matter the University or anyone on its behalf collects, accesses, maintains, distributes, processes, protects, stores, uses, transmits, disposes of, or otherwise contains personally identifiable information.

4. Process of Confirmed theft, data breach or exposure of BGU protected data or BGU sensitive data

4.1. This policy requires that any individual who suspects that a theft, breach or exposure of University Protected data or University Sensitive data has occurred must immediately provide a description of what occurred via e-mail to databreach@bishopg.ac.uk This e-mail address is monitored by the University’s Quality and Governance department.

4.2. As a minimum, when reporting a potential breach, the following will need to be communicated:

- your name and contact details;
- the estimated date of the breach;
- a summary of the incident, to include where possible;
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- the nature and content of the personal data;
- the likely effect on the individual;

- any measures you have taken to address the breach; and
- how they can mitigate any possible adverse impact.

A Data Breach Incident Reporting Form is included in Appendix A.

4.3. As soon as an alleged theft, data breach or exposure containing protected data or sensitive data is reported and identified the Governance Office will initially investigate the alleged breach. If the breach occurs within the Governance Office, the Data Protection Officer will appoint a nominee to investigate the matter.

4.4. If the breach is confirmed then the Data Protection Officer (or nominee) will chair an incident response team to handle the breach or exposure. The process of minimising impact of the breach will begin and run in parallel.

Membership of the incident response team will be determined according to the nature of the breach involved, including (as required) representatives from:

- Registry (including the Data Protection Officer or their nominee)
- IT Services
- Data Stewards/Owners
- Marketing and Communications
- Human Resources
- Additional departments based on the data type involved.
- Additional individuals as deemed necessary by the chair.

4.5. The Governance Office will ensure a breach log is kept containing:

- a description of the nature of the personal data breach
- a description of likely consequences of the personal data breach
- the measures taken or proposed to be taken to address the personal data breach

4.6. If required, the incident response team will work with Forensic Investigators to determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organisations impacted; and analyse the breach or exposure to determine the root cause.

The incident response team will work with Marketing and Communications to decide how best to communicate the breach to: a) ICO, b) internal employees, c) the public, and d) those directly affected. The response, if required, will occur no later than 72 hours after the breach is initially reported. The communication method will be signed off by the chair of the Data Protection Officer/nominee.

5. Ownership and Responsibilities

Roles & Responsibilities for implementation of this policy:

- Chief Operating Officer – accountable for the oversight and implementation of this policy
- Data Protection Officer (nominated as the Registrar) – responsibility for ensuring actions are carried out in accordance with this policy;

- Data Stewards/Owners - members of the University community that have primary responsibility for maintaining any particular information resource, as noted in Appendix B. Data Stewards/ Owners are required to ensure any breaches in their area of which they become aware are immediately reported through the procedures noted in this policy and form part of the incident team to investigate any such incidents.
- Information Technology Services - the department of the University who provides administrative support for the implementation, oversight and coordination of all IT procedures and systems;
- All University staff with access to data – to ensure they are informed as to the content of this policy and aware of the procedures to be followed should they determine a data breach has occurred in their area.

5.1. Users of the policy include all members of the University community to the extent they have authorised access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.

6. Enforcement

Any University personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

7. Revision History

Version	Date of Revision	Author	Description of Changes
1.0	June 2017	Director of IT	Initial draft
1.2	June 2018	Information Compliance Officer	Housekeeping update

Appendix A: Data Breach Incident Reporting Form

NAME OF PERSON REPORTING:	**DATE OF BREACH OCCURRING:** **TIME:**	**DATE ON WHICH BREACH WAS DISCOVERED:** **TIME:**
SCHOOL/DEPARTMENT:		
EXTENSION NUMBER/CONTACT NUMBER:		
	DETAILS OF THE DATA BREACH	
How did the breach occur?	*Please provide as much information as possible:*	
Has a breach of this nature occurred before within the School/Department?	*If so, please provide dates of any previous breaches of the same nature:*	
How many individuals does the data breach affect?	*Please, aim to provide a figure as accurate as possible:*	
Are the individuals affected by the breach students/staff, or both?		
What data has been lost/stolen/compromised or else disclosed without the appropriate authority?	*i.e. CVs, Financial Information, Contact details etc.:*	
How many personal data records does the data breach affect?	*Please, aim to provide a figure as accurate as possible:*	
Whom was the data released to, if known?		
Is the data sensitive? YES/NO	*If YES, please provide a list of sensitive data concerned:*	
Are you aware of the individuals affected?	*If so, please provide their names and any contact details, where known:*	

What steps could those individuals take to protect themselves from any harm/risk arising from the breach?	*i.e. report to their bank/building society, report to the Police etc.:*
Have you taken steps to address the data breach?	
Does the breach concern manual or electronic data, or both?	
Were encryption protections in place at the time of the breach?	
Have the IT Services been informed?	*If your account has been hacked, you must change your password immediately and report the incident to IT Services:*
Has the incident been reported to the Police or any other authorities?	*If so, please provide date of reporting and reference number:*
IS THERE ANYTHING ELSE THE UNIVERSITY SHOULD BE AWARE OF?	
Please comment below:	
THIS FORM MUST BE SUBMITTED TO databreach@bishopg.ac.uk	

Appendix B: Data Stewards/Owners

To follow

VERSION:	**1**	**AUTHOR/ OWNER:**	**Chief Operating Officer**
Approved Date:	xxxxxxxxx	**Approved By:**	xxxxxxxxxxxx
Review Date:	xxxxxxxxx		