Procedure for reporting incidents that potentially lead to a data breach

Organisation	Leeds Beckett University
Author(s)	Head of Information Governance
Developed in consultation with	Records and Information Governance Manager Information Compliance and Data Protection Manager
Owner	University Registrar and Secretary's Office
Target audience	Staff, Students, Data Processors
Sensitivity	Public
Approved by	Information Compliance Team Meeting
Endorsed by	IMOG
Effective date	22nd June 2022
Review Date	+2 years from last date of approval [08-2024]
Status	Published
External references	
Links to other internal policies / procedures	Information Governance Framework
Version reference	2.0
Version history and summary of changes	1.0, first published version. *Modified to make the focus on incident reporting instead of data breach reporting. Removal of training material with links to short guides.*

Introduction

The objective of this procedure is to enable staff to act promptly to contain any incidents and/or breaches that occur, minimising the risk associated with the potential breach or incident and take action if necessary, to secure personal data and prevent further risk.

This procedure applies to all staff, students, partners, governors, employers, suppliers or third parties we work with. It should be read in conjunction with the university's Data Protection Policy available on the Information Governance Policies website page. This policy states that "*all personal data must be processed in accordance with this policy and the Data Protection Act 2018 (DPA) and the General Data Protection Regulations 2016 (GDPR) or any successor legislation to the GDPR or the DPA. Failure to comply may result in disciplinary action or even criminal proceedings.*"

Every care is taken by the university to protect information/data from situations where a breach could compromise the data protection principles which are:

- **lawfulness, fairness and transparency –** identify lawful basis for processing – only shared legally (lawfulness), not adversely impact individuals (fairness), informing individuals/privacy notice (transparency)
- **purpose limitation –** only being used for a specific purpose
- **data minimisation –** minimum personal data to carry out what is required
- **accuracy –** accurate and reliable information
- **storage limitation –** only held for specified purpose with set storage and retention requirements
- **integrity and confidentiality (security) –** data quality, processed securely with authorised/approved access

The university must report a significant breach, that is likely to impact on data subjects' rights and freedoms, within 72 hours to the **Information Commissioner's Office (ICO).** Failure to report promptly to the ICO could result in enforcement action.

If you become aware of a data breach it is essential that you report it immediately so that the university can assess the situation and take prompt action to limit or prevent any potential harm or damage.

What is an incident?

An incident is any occurrence involving information that contains personal data which presents a risk to the security of the information, leading to the: accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the purposes of the university's business.

What is a breach?

An incident that may be determined as a breach of personal data breach includes, but is not restricted to, the following:

- Loss of data or equipment (including equipment failure) on which personal or sensitive data is stored, for example; loss of laptop, USB pen, iPad/Tablet device, or paper record. This could be caused by unforeseen circumstances such as fire or flood.
- Inappropriate access (includes inappropriate access controls, allowing unauthorised access by Staff/Colleagues)
- Unauthorised external access (Includes; theft, hacking, access by deception)
- Unlawful alteration or destruction (Includes malicious acts performed by Colleagues/Contractors)
- Unauthorised disclosure of sensitive/personal data (i.e. email to wrong individual, organisation)

An investigation with the Information Governance team will assist in determining whether an incident has become a breach and help assess the seriousness/harm it could cause and actions to be undertaken.

A breach in IT security or an external threat to university networks or systems should also be documented and investigated in the same way. Where you are uncertain if the incident constitutes an IT security incident please call the IT service desk and Information Governance.

Incident Reporting

In the first instance, you should report an incident to the Information Governance team.

Staff and Colleagues should also report the incident to their line manager and/or Information Asset Owner/Risk Manager.

Method of reporting

All incidents must be reported to the Information Governance Team through either the online webform or using the incident reporting form which can be found on the Information Governance short guides webpage provided by Information Governance or by emailing the Data Protection Officer (DPO) via dpo@leedsbeckett.ac.uk

Acknowledgement

The DPO will acknowledge receipt of the reported incident promptly. If you do not hear from the university's DPO within 24 hours, please contact the Information Governance team and/or re-send details of the incident as there may have been a technical failure.

Our contact information is published at https://www.leedsbeckett.ac.uk/our-university/public-information/information-compliance/contact-us/

Investigation

The procedure below is set out provides you with the steps you need to take to enable you identify when a breach has taken place and what the action should be. The Information Governance Team have produced a process map to assist.

a) Identify the right people

The IG team will work with Schools and Services to identify the appropriate investigation lead(s) which will normally be an Information Asset Owner and/or system owner. Where the information cuts across a variety of schools and services this could involve a team of multiple leads to address each area.

b) Access the risk

Working with all leads and the Information Governance team the risk will be assessed and recorded in accordance with published guidance (See Appendix 1). As the investigation is undertaken the risk may subside or increase but the initial assessment is to understand where we may be required to report to the ICO.

c) Completing the investigation

Following the initial risk assessment, a more thorough investigation will be undertaken. The nominated lead will investigate the breach using the investigation form and liaise with the Information Governance Team. All completed forms and materials captured as part of the investigation should be returned to the Information Governance Team for managing in line with the university retention schedule.

d) Assigning action(s) arising from the investigation

Following immediate containment, the risks which may be associated with the breach, potential adverse consequences to the individuals, as well as the university itself, and the seriousness of the breach must be assessed. Please use the risk assessment form which can be found on the Information Governance short guides webpage.

For risk requiring actions over a medium/longer term these will be agreed through the development of an action plan in collaboration with the Information Governance Team and the School /Service Information Asset Owner (IAO) who will be responsible for satisfactory closure.

e) Notification

Internal - Dean, Director, SIRO, External Relations, Legal, Insurance, Human Resources

External – police, Information Commissioners Office (ICO), stakeholders (Office of Students, JISC, Student Loans) our partners (contractors, joint controllers and processors)

Where you are considering alerting any external bodies, communicating wider and/or reporting information relating to a breach this would be led by the DPO/Head of Information Governance and the Senior Information Risk Office (SIRO) (delegated to Deans and Directors where appropriate).

f) Monitoring and auditing of agreed actions

The Information Governance team will ensure that the incidents are captured on the university incident register. The team will monitor agreed actions and work with the owner to ensure their completion and or satisfactory closure.

Lesson learnt

Relevant lessons learnt will be fed back to the service and/or school to implement the required changes and or guidance or training. Lessons learnt will be fed into:

- the Information Management Operational Group (IMOG) where required.
- the DPO forum for discussion to influence informal change at the service level meetings.
- the Strategic Data Management Group (UET/ SDMG for strategic change).

Where serious incidents and or breaches have occurred lesson may be shared more widely.

Any risks signed off and associated actions will be maintained by the SIRO, in a risk log by the Information Governance team and made available to IMOG members as needed.

For the purposes of this procedure data breaches include both confirmed and suspected incidents.

What should be considered upon discovering a data breach?

- The type of data involved
- Its sensitivity
- If data has been lost or stolen, whether data has been protected by encrypted devices or software
- What has happened to the data, such as the possibility that it may be used to cause harm to the individual(s)
- Who the individuals are, number of individuals involved and the potential effects to those data subject(s)
- Whether there are wider consequences to the breach
- Whether any actions have been taken during the breach that contravene the policies, procedures and training in place.

What do you do if you discover a data breach?

It's important that you play a part in reporting the breach. For university employees a failure to follow the correct procedure or ignoring a possible data breach could result in disciplinary action. Where a breach has occurred, all employees are encouraged to report it. This will enable the Information Governance team to support your school /service in containing the breach and implementing appropriate actions.

1. NOTIFYING A SERIOUS DATA BREACH TO THE INFORMATION COMMISSIONER'S OFFICE (ICO)

Where an investigation outcome determines the breach is significant, the notification will be drafted by the Information Compliance Team and DPO, and any notification to the ICO must only be made by the DPO. **Please be aware you must not try and deal with a serious data breach yourself. The decision as to whether any third parties need to be notified will be made by the Information Compliance Team, our DPO and senior management.**

2. EVALUATION AND RESPONSE

The key to preventing further incidents is to ensure that the university learns from previous incidents.

It is extremely important to identify the actions that the university needs to take to prevent a recurrence. Our DPO and senior management will carry out an evaluation as to the effectiveness of our response to the data breach and document this in our Data Breach Register. Senior management may then make changes to University procedures to minimise the likelihood of incidents occurring again. Lessons learned and good practice will be shared/disseminated via IMOG

Definitions

Personal data:
If the data 'relates to' the identifiable living individual, whether in personal or family life, business or profession, then it is Personal Data.

Special category personal data:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- Biometric data (where used for identification purposes);
- Data concerning health;
- Data concerning a person's sex life; and
- Data concerning a person's sexual orientation.

Sensitive personal data:
A term used to Include special category data but can have a wider scope to include other personal data which could cause significant harm in some circumstances. This

can include young person data, criminal data and data relating to vulnerable persons such as those fleeing domestic violence.

APPENDIX 1

Guidance - Checklist for data breaches

The guidance outlines actions and considerations when addressing a data breach. All breaches must be notified to the Information Compliance Team whom will provide guidance on the checklist and managing the breach.

Step	Action points	Notes
Containment and recovery **To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**		
1	Establish school/service lead for reporting breach to Information Compliance Team and investigating the breach.	To investigate extent and nature of breach, to contact and co-ordinate with specialists and stakeholders (e.g. School or Service Managers, Information Asset system owners, External Relations, Information Compliance Team, IT Services).
2	Ascertain the scope of the breach and if any personal data is involved.	See 'Risk assessment' below.
3	Establish who needs to be made aware of the incident within the school/service and inform them of what they are expected to do to assist in the containment/ recovery exercise.	E.g. This may require actions such as the deletion of miss sent email and data, finding lost piece of equipment, changing passwords or access codes, or may isolating/closing part of network, pulling webpages, informing police, checking any contractual obligations to act/report where data has been supplied under contract. If you have any reason to suspect that there is computer misuse ("hacking"), contact the IT Service Desk who will provide advice.
4	Ensure that any possibility of further data loss is removed or mitigated as far as possible.	As above and may also involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.

5	Determine whether anything can be done to recover any losses and limit any damage that may be caused.	E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups. E.g. stolen property, fraudulent activity, offences under Computer Misuse Act and reporting to police.
Risk assessment **To identify and assess the ongoing risks that may be associated with the breach. In particular an assessment of:** **(a) potential adverse consequences for individuals,** **(b) their likelihood, extent and seriousness.** **Determining the level of risk will help define actions in attempting to mitigate those risks.**		
6	What type and volume of data is involved?	
7	How sensitive is the data?	Personal or special category data? Or sensitive because of what might happen if misused (banking details).
8	What has happened to the data?	E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relates; if it has been damaged, this poses a different type and level of risk.
9	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.
10	If the data was damaged/ corrupted/ lost, were there protections in place to mitigate the impact of the loss?	E.g. back-up/copies.

Additional assessment for breaches involving personal data		
11	How many individuals' personal data are affected by the breach?	Collate number of individuals.
12	Who are the individuals whose data has been compromised?	Students, applicants, staff, customers, clients or suppliers?
13	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
14	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to: physical safety; emotional wellbeing; reputation; finances; identify (theft/fraud from release of non-public identifiers); or a combination of these and other private aspects of their life?
15	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide? Did any action that took place contravene policies, procedures and training in place and as a result caused the data breach? Does this action require further investigation? Does the outcome of the investigation require invoking of the disciplinary procedure or criminal proceedings?

Notification		
16	Are there any legal, contractual or regulatory requirements to notify?	Report breach and liaise with the Information Governance Team and University Secretary (Data Protection Officer) whom will deal with legal, contractual or regulatory requirements to notify. E.g.: OfS Reportable Events Procedure; contractual obligations; obligations under Legal requirements such as Data Protection Act 2018, GDPR, Privacy and Electronic Communications Regulations, Computer Misuse Act
17	Notifying individuals where it is one or a small number of individuals - consider what you will tell them and how you will communicate the message.	There are a number of ways to notify those affected, consider using the most appropriate one and that a phone call is a more personal way of communicating what has happened. Always bear in mind the security of the medium as well as the urgency of the situation. Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. Where necessary give specific and clear advice on the steps they can take to protect themselves (e.g. by changing a password).
18	If a large number of people are affected, or there are very serious consequences.	Report and liaise with the Information Governance Team and University Secretary (Data Protection Officer) whom will contact the ICO where appropriate with regards notification of breach requirements and provided guidance on actions required. The content of the notification will be drafted by our DPO in conjunction with consulting the ICO where necessary.

		Please be aware that **under no circumstances must you try and deal with a serious data breach yourself.**
Evaluation and response **To evaluate the effectiveness of the University's response to the breach. To learn and apply any lessons or remedies in the light of findings or experience.**		
19	Establish where any present or future data protection and security risks lie.	Review and discuss incident investigation, findings and conclusions at Team Meetings, incorporate changes and improvements to work practices. Consider any actions that contravene the policies, procedures and training in place and caused the data breach.
20	Consider the personal data and contexts involved.	E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept) where are the weaknesses and how can they be mitigated.
21	Consider and identify any weak points in existing data protection and security measures and procedures.	E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.
22	Consider and identify any weak points in levels of data protection and security awareness/training.	Fill any gaps through training or tailored advice.
23	Consider and identify any action that took place that contravened data protection and security policies, procedures and training in place and as a result caused the data breach.	Fill any gaps through updated policies training or tailored advice. Raise awareness of the consequences of any contravening of policies, procedures and training.