DATA BREACH PROCEDURE

Organisation	Leeds Beckett University
Author(s)	Head of Information Governance
Developed in consultation with	University Secretary Records and Information Governance Manager
Owner	University Secretariat Office
Target audience	Staff
Sensitivity	Public
Approved by	Information Compliance Team Meeting
Endorsed by	IMOG
Effective date	16-07-2020
Review Date	+2 years from last date of approval [08-2022]
Status	Published
External references	
Links to other internal policies / procedures	Information Governance Framework
Version reference	1.00
Version history and summary of changes	No previous versions.

Every care is taken by the University to protect personal data from situations where a data protection breach could compromise 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

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 Data Protection 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*."

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

The University expects its staff to comply with and embed data security practices in their normal working day to ensure personal, or special category, data is protected and must take appropriate steps to safeguard this information.

Under the **Data Protection Act 2018 (DPA)** and the **General Data Protection Regulation 2016 (GDPR)** the University must report any 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 substantial fines.

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

In the first instance, you should report a breach to your line manager, your School or service data protection contact and Governance & Legal Services.

The procedure below is set out to help you identify when a breach has taken place and what the action should be.

What is a data breach?

A personal data breach is 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 in connection with the purposes of the University's business.

A breach in IT security or an external threat to University networks or systems should also be documented and investigated in the same way.

A personal data breach includes, but is not restricted to, the following:

- Loss or theft of data or equipment on which personal or sensitive data is stored (i.e. loss of laptop, USB pen, iPad/Tablet device, or paper record)
- Inappropriate access controls allowing unauthorised access and/or use
- Inappropriate access
- Equipment theft or failure
- Unforeseen circumstances such as fire or flood
- Hacking attack
- Human error
- Unlawful alteration or destruction
- Offences where information is obtained by deceiving the holder of the information
- Unauthorised disclosure of sensitive/personal data (i.e. email to wrong individual, organisation)

What is Personal Data?

Definition of personal data:
Can a living individual be identified from the data, or, from the data and other information in your possession? If the data 'relates to' the identifiable living individual, whether in personal or family life, business or profession, then it is Personal Data.

Definition of 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.

What type of Personal Data does the University use or process?

We collect, process and hold **Personal Data from Students** on their Application and Enrolment forms, which we then input into the University student record systems. This includes information such as their name, contact details, date of birth, parent/guardian or emergency contact, ethnicity, learning difficulties and disabilities, health information, criminal convictions (if applicable), their photo (for their ID card). We may also collect payment details if the student is paying for their course.

The information we record whilst the student is studying with us is also considered Personal Data. This is used to monitor their progression, attendance, behaviour, target grades, assessments, and any support that's needed. University staff also use students' personal data every day in registers and class lists.

We collect, process and hold **Personal Data from Staff** as they complete the recruitment process and in relation to their employment contracts. Each staff member will have an employee file and an electronic record held on our central HR system. This includes information such as their name, contact details, date of birth, NI number, next of kin, bank details, pension details, certifications/qualifications, employment terms and conditions. The University also records information relating to sickness absence and any incidents or disciplinary action that have occurred during their employment.

We collect, process and hold **Personal Data and Financial Data about our Partners, Governors, Employers, Suppliers and Third-Party Organisations**. Although the amount of information we hold on individuals may be minimal, and may relate to their business or profession, if they are identifiable as a living individual it still counts as Personal Data.

The information we collect may be on paper, stored in emails and/or electronic files or stored within systems, but all formats constitute part of the individuals Personal Data, and as such must all be protected by University employees against a breach occurring.

How do I access the risk?

Some data breaches may not lead to risks beyond possible inconvenience to those who need the data to undertake their role. Following immediate containment, the risks must be assessed 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 considered, further to immediate containment

Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the University is able to quickly identify the classification of the data and assess the risk to data subjects or the University.

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.

What do you do to report a data breach?

If you become aware of a data breach and have a reasonable degree of certainty, that a data breach or security incident has occurred, you must report this to our **Information Compliance Team** immediately. We have a legal obligation to keep a register of all data breaches.

False alarms, near misses or even breaches that do not cause any harm to individuals or to the University should be reported as it will enable the University to learn lessons and consider remedial action that can be put in place.

Breaches can be inputted on the Report a Data Breach Form available on the Data Protection page and sent via email for their attention to: infocompliance@leedsbeckett.ac.uk

When you report a data breach to the Information Compliance Team or University Secretary as Data Protection Officer (DPO), they will support the investigation into the breach, to ascertain the seriousness of the breach to ensure the University complies with the 72-hour deadline to report any **serious data subject or security breach** to the ICO that may impact on data subjects or result in a risk to the rights and freedoms of individuals.

INFORMATION COMPLIANCE TEAM SERIOUS DATA BREACH ACTIONS

1. ASSESSING A SERIOUS DATA BREACH

Once the level of severity is identified as a serious data breach our Information Compliance Team or DPO will notify management. Depending on the severity, a response team may need to be appointed, which may involve for example our HR and IT Teams who may be assigned responsibility for particular tasks as necessary across the response team.

If our Information Compliance Team, DPO and management consider that the breach is very serious, they will consider the impact on our reputation and the effect it may have on the trust placed in us. We will then continue to investigate the breach and consider any on-going risks to the individuals affected.

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

Where the incident is likely to result in having a serious impact on data subjects or result in a high risk to the rights and freedoms of individuals, the University **must** notify the breach to the ICO within 72 hours of becoming aware of the breach.

The content of the notification will be drafted by our Information Compliance Team and DPO, and any notification to the ICO must only be made by the DPO.

3. NOTIFYING A SERIOUS DATA BREACH TO INDIVIDUALS

We must also notify the individuals concerned as soon as possible to inform them of the incident and the actions that have been taken to address the incident. The content of the notification will be drafted by our DPO in conjunction with consulting the ICO where necessary.

We will notify individuals in clear and plain language and in a transparent manner.

Please be aware that **under no circumstances must you try and deal with a serious data breach yourself.**

4. NOTIFYING A SERIOUS DATA BREACH TO OTHER RELEVANT THIRD PARTIES

We may also consider that it is necessary to notify other third parties about the data breach depending on the nature of the breach. This could include:

• Insurers • Police • Parents/Guardians • Regulator	• Sponsors • Banks • Contract counterparties

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.

5. UPDATING NOTIFICATIONS

We need to keep the ICO up to date about the data breach. If anything changes from the time, we send the initial notification to the ICO, our DPO will consider whether we need to update the ICO about the data breach.

6. 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 of the incident. 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.

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 Compliance 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 Compliance 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.