Data Protection Breach Policy

Table of Contents

A. Purpose

The University is required under the data protection legislation to have in place robust breach detection, investigation and internal reporting procedures. This policy describes the steps that will be taken to investigate and respond to potential data protection breaches in order to minimise the risk of harm to individuals and the reputation of the University.

B. Scope

What information does the policy apply to? The policy applies to all information held by the University both in electronic and hard copy formats.

Who does the policy apply to? All staff of the University.

C. Understanding and identifying a Data Protection Breach

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.

Examples of incidents that could result in a data protection breach include (but not restricted to):

- Unauthorised disclosure of personal information to external parties (either accidental or deliberate).
- Information sent in error to an unintended recipient.
- Phishing attacks that have resulted in personal information disclosure or disclosure of access details to University systems.
- Loss or theft of devices on which University personal data is stored (e.g. laptops and tablets).
- Loss or theft of hard copy materials including personal data.
- Hacking attacks of University systems.
- Equipment failure resulting in a loss of data.

Published date: June 2023
Review date: May 2024

D. Reporting a Confirmed or Suspected Data Protection Breach

All staff are required to act promptly to notify the University of a breach or suspected breach to ensure that the incident is contained quickly.

Staff should notify both their head of department and IT helpdesk as soon as the incident is identified. IT helpdesk will record information about the incident and take steps to contain the incident where possible in relation to incidents involving IT systems security. Where personal data has been lost through other breaches such as human error or lost paperwork other staff will be notified to further investigate the impact of the incident.

Staff involved need to ensure they respond to further requests for information as soon as possible whilst activity takes place to understand the risk from the incident reported.

E. Incident Investigation

For breaches resulting from IT security based incidents the investigation will be led by appropriate staff in IT services. Non-IT security based incidents investigations will be led by the Data Protection Officer. A Data Protection Breach Panel will be notified of the investigation and approve the resulting action that is required.

If a breach is confirmed to have occurred the University will take action to:

- Ensure all appropriate steps are taken to contain the breach.
- Ensure affected data subjects have been notified where appropriate.
- Create a record of the incident
- Assess if staff training or procedures require improvement to prevent repeat incidents.
- Assess if any system security issues need to be strengthened.
- Investigate whether individual staff should be subject to any disciplinary action in the event of serious breaches resulting from poor adherence to expected standards.

F. Incident reporting to the ICO

The University will act to comply with data protection legislation to notify the ICO of reportable incidents within the required timescale of 72 hours from being aware of the breach. The university will assist the ICO as required. This action will be led by the Data Protection Officer and reported to the Data Protection Breach Panel. Other staff may be required to support this activity and will be expected to comply with this without delay.

G. Breach register

On completion of the investigation the Data Protection Officer will update the University's data protection breach register to record the details of the incident and action taken.

H. Evaluation and review

This policy will be formally reviewed every year by the Data Protection Officer. In addition, the effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.

This policy was last updated in May 2023.

Published date: June 2023
Review date: May 2024