Personal Data Breach Procedure

1 Introduction

This procedure should be followed in the event of a breach of personal data. Where breaches are large, or if you have reason to believe a large amount of personal data could have or has been breached, or if very sensitive data has been lost, e.g. data on students' health conditions, the Information Compliance Team will also inform Digital and Technology Services.

If you need guidance, please contact the Information Compliance team via data-protection@nottingham.ac.uk. For technical assistance, contact the DTS Service Desk.

2 Aim

This procedure standardises the University-wide response to reported personal data breach incidents, and ensures that they are appropriately logged and managed in accordance with best practice guidelines and relevant UK data protection laws.

3 Definitions

Personal data is defined as *'*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (*UK GDPR*)

'A *personal data breach* can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.' *(Information Commissioner's Office website)*

4 Responsibilities

All information users are responsible for reporting actual, suspected, threatened or potential information security incidents, which includes personal data breaches. Any unmitigated breach that affects the rights and freedoms of an individual must be reported to the ICO by the Information Compliance Team no later than 72 hours after the University becomes aware of it, so prompt reporting is essential.

5 Communication

This procedure will be published on the Information Compliance and Security Sharepoint site. Line managers are responsible for bringing this procedure to the attention of staff in their area, including new starters.

6 Revision

This procedure will be revised regularly, and formally approved by the Information Management and Security Steering Committee.

Approved: 21 May 2018
Revised Nov 2021
Next revision due: Jan 2023

7 Contact

Tracy Landon

Associate Director of Information Compliance, Governance and Assurance Central, Data Protection Officer
Tracy.Landon@nottingham.ac.uk

University of Nottingham
UK | CHINA | MALAYSIA

Procedure for managing a data breach

1 Reporting data breaches

All data breaches should be reported using the form here which will be sent to University's Information Compliance Team, who can be reached at data-protection@nottingham.ac.uk. Please do not perpetuate the breach by forwarding the breached material itself.

If you need to report a breach outside normal working hours, please call the IS Service Desk on 0115 9516677.

All data breaches will be logged and where appropriate, reported to the Information Commissioner's Office by the Information Compliance Team.

2 Further steps to take

- Please try and rectify or contain the breach as best you can. The Information Compliance Team can offer support with this.
- Where individuals have received the personal data of others in error, they should be apologised to, be asked to delete the material without sharing it further, and be asked to confirm the deletion of the material. Further guidance including a template email to send to the recipient asking for their assistance is available Information Security & Compliance SharePoint site.
- Liaise with the Information Compliance Team to determine whether it is appropriate to notify the affected data subject that a breach has occurred. If appropriate, the data subject should be apologised to and notified of the nature of the data breach. A template email to send to the individual whose data has been breached can be also be found in the previously linked document.