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 the Information Security Team. If you need guidance, please contact the Information Compliance team via data-protection@nottingham.ac.uk.

2 Aim

This procedure standardises the University-wide response to any reported personal data breach incident, and ensure that they are appropriately logged and managed in accordance with best practice guidelines and the General Data Protection Regulation and all relevant data protection law.

3 Definition

'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 notifiable breach must be reported to the ICO without undue delay, but not later than 72 hours after the University is aware of it, so prompt reporting is essential.

5 Communication

This procedure will be published on the University's internal website. Line managers are responsible for bringing this policy to the attention of members of staff in their area, including new staff.

6 Revision

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

Approved: 21 May 2018

Next revision due: June 2020

7 Contact

Sara Smith
Head of Information Compliance
Sara.J.Smith@nottingham.ac.uk

Procedure for managing a data breach

1 Reporting data breaches

All data breaches should be reported using the form here and emailed to the University's Information Governance 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 email the breach form to the IT service desk at itservicedesk@nottingham.ac.uk.

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

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 here.
- 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.