Nottingham Trent University

Governance and Legal Services

Data Breach Policy and Procedure

Version: 2
Date: August 2022

Version: 01 New Policy
Date: May 2018
Approval: UET
Author: DPO
Next Review: 2021/2022

Version: 02
Date: August 2022
Approval: UET
Author: DPO
Next Review: 2023/2024

Contents

1. Introduction

A “Personal Data Breach” is defined as “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”.

The UK General Data Protection Regulation (UK GDPR) introduces a duty on all organisations to report certain types of Personal Data Breaches to the relevant authority.

This Data Breach Policy (this Policy) sets out how Nottingham Trent University (NTU) identifies and manages its Data Breach responsibilities in accordance with its legal and regulatory obligations. It also sets out the minimum standards which must be complied with by NTU. A Personal Data Breach Workflow is provided at 9. Appendix (page 6).

See NTU’s Data Protection Policy for an explanation of what is meant by “Personal Data” and “Special Category Personal Data”, and what “Processing” Personal Data means.

2. Scope

This Policy applies to the entirety of NTU employees, students and where appropriate third parties working for, or on behalf of NTU. This applies to all data relating to identifiable individuals.

3. Regulatory Requirements

This Policy has been documented giving consideration to, and in compliance with the following regulatory requirements.

Regulatory Requirement	Status
Retained UK version of the General Data Protection Regulation ((EU) 2016/679) as defined in the Data Protection Act 2018 (UK GDPR)	UK Legislation
The Data Protection Act 2018	UK Legislation
Information Commissioner’s Office (ICO)	UK Independent Body and data protection regulatory / guidance

4. Responsibilities

4.1 University Executive Team (UET)

UET has overall responsibility to ensure NTU meets its legal and regulatory responsibilities under the UK GDPR, and to ensure compliance with this Policy.

4.2 Employees

All employees are responsible for raising any potential or actual data breaches to the Data Protection officer (DPO) or the Information Governance Manager at DPO@ntu.ac.uk.

It is the responsibility of all employees to ensure that they have read and understood this Policy and raise any concerns with non-compliance to the DPO.

4.3 Legal Services

This Policy is owned by the Legal Services Team,. Legal Services has the right to escalate any issues of non-compliance with this Policy to the DPO who may in turn escalate to UET should that be appropriate. The DPO can be contacted by emailing DPO@ntu.ac.uk.

5. What is a Personal 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, whether by accidental or deliberate causes.

5.1 Examples of Personal and Special Category (sensitive) Personal Data

Personal Data	Special Category (sensitive) Data
Full Name	Racial or ethnical origin of the data subject
Date of Birth	Political Opinions
Address / email address	Religious beliefs or beliefs of a similar nature
Postcode	Whether the data subject is a trade union member
Telephone / mobile numbers	Physical, mental health or condition
Bank Details	Sex life or sexual orientation
Employee / Student ID number	Commission or alleged commission of any offence
Driving Licence / Passport number	Any proceedings for any committed or alleged offence, including the disposal or sentence of any court in such proceedings
National Insurance Number	

5.2 Types of breaches and categories

Personal Data Breaches can include (but are not limited to):

- access to personal data by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient (email or otherwise);
- hand-held devices / laptops containing personal data being lost or stolen;
- alteration of personal data without permission;
- paper documents which contain personal data which is not locked away (ie left on a desk in an open office); and/or
- loss of availability of personal data.

There are three categories of Personal Data Breaches:

- "***Confidentiality breach***" - where there is an unauthorised or accidental disclosure of, or access to, personal data; or
- "***Integrity breach***" - where there is an unauthorised or accidental alteration of personal data; or
- "***Availability breach***" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

5.3 Practical examples of Personal Data Breaches

- I have lost a USB stick which I was using, which holds personal information;
- My work laptop has been stolen (from work or elsewhere);

- I sent an email/spreadsheet containing data to the wrong person (staff, student or external);
- I sent a letter/email including someone's bank details to an incorrect address/email address;
- I updated a student's address and mobile number, but it was on the wrong student profile; and/or
- I printed a document which contained personal data, left it on a desk and now I cannot locate it.

6. Obligations

All employees and those who are engaged formally to work for, or act on behalf of, NTU have a contractual obligation to take adequate steps to prevent unauthorised use or disclosure of personal data.

The protection of personal data is a legal obligation imposed by the UK GDPR. The UK GDPR requires adequate steps to be taken to protect personal data, with even greater care expected to protect sensitive personal data (Special Category Personal Data) in view of its private nature.

7. Reporting a Personal Data Breach

Any incident or breach concerning personal data should be escalated to the DPO, as soon as possible and within 24 hours of the incident/breach coming to your attention.

To report a breach please use the data incident form on the GDPR pages on MyHub under ***"Reporting a data incident".***

The DPO and/or the Information Governance Manager will investigate and make the decision as to whether an escalation to the Information Commissioner's Office (ICO) is required.

If a Personal Data Breach is likely to result in a risk of harm to the individuals concerned, then the DPO must report this to the ICO without delay, and at the latest within 72 hours and must include, amongst other things, details of the data subject and whether the breach might pose a high risk to their rights and freedoms.

All evidence relating to a potential Personal Data Breach should be preserved, including, but not limited to, emails or other correspondence, logs or screen shots, and the breach form, should be completed with as much detail as possible.

Failure to report a Personal Data Breach in accordance with this Policy could lead to disciplinary action. Compliance with this Policy is critical to ensure that any Personal Data Breach is dealt with carefully and promptly to protect the personal data of data subjects.

Violations regarding record-keeping, security, breach notification, and privacy impact assessment obligations, can result in a penalty of up to £8.7 million or 2% of global gross revenue, whichever is greater.

More serious violations related to lawful processing of personal data such as consent, data subject rights and cross-border data transfers, can result in a penalty of up to £17.5 million or 4% of global gross revenue, whichever is greater.

8. Contact details

If you are unsure of whether something is a personal data breach, please get in touch with the DPO / Information Governance Manager to discuss.

Please contact the DPO / Information Governance Manager with any queries.

Contact us at:
DPO@ntu.ac.uk

9. Appendix: Personal Data Breach Workflow