Governance and Legal Services

Data Breach Policy

NOTTINGHAM TRENT UNIVERSITY | 50 Shakespeare Street, Nottingham, NG1 4FQ

NOTTINGHAM TRENT UNIVERSITY

Version Control

Document Reference:	GDPR002
Policy Owner:	Governance and Legal Services
Approval Committee:	University Executive Team (UET)
Version:	Version 1
Next Review Date:	May 2019

Policy History

Version:	Author:	Reason for Issue:	Date:
Version 1	Legal Services	New Policy	23 April 2018

Contents

1. Introduction

A 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 General Data Protection Regulation (GDPR) introduces a duty on all organisations to report certain types of personal data breach to the relevant authority.

This Policy sets out how Nottingham Trent University (NTU) identifies and manages its Data Breach responsibilities in accordance with its legal and regulatory obligations.

This Data Breach Policy sets out the minimum standards which must be complied with by NTU.

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.

Body	Regulation	Section / Paragraph
General Data Protection Regulation **(GDPR)**	Regulation	All
Information Commissioner's Office **(ICO)**	UK Independent Body/ Guidance	GDPR and FOI
The Freedom of Information Act **(FOI)** 2000	Regulation	All

4. Responsibilities

University Executive Team
The University Executive Team (UET) has overall responsibility to ensure NTU meets its legal and regulatory responsibilities under GDPR, and to ensure compliance with its Policy.

Employees
All managers and employees are responsible for raising any potential or actual data breaches to the Data Protection Officer (DPO).

It is the managers and employees responsibility to ensure they have read and understood this policy, and raise any concerns with non-compliance.

Legal Services
This Policy is owned and set by the Legal Services Team, which includes the DPO. The Legal Services Team has the right to escalate any issues of non-compliance with this Policy to UET.

5. 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.

Personal data breaches can include (but 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);
- loss of availability of personal data.

There are three categories in which breaches can be sectioned:

- "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.

6. Guidance

All NTU employees and those who are formally engaged to work or act on behalf of the University 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 GDPR. The GDPR requires adequate steps to be taken to protect Personal Data, with even greater care expected to protect Sensitive Personal Data in view of its private nature.

7. Escalation

Any incident or breach concerning personal data should be escalated to the Data Protection Officer (DPO), as soon as possible and within 24 hours of the incident/breach coming to your attention, using the form within the Data Breach Procedure. The DPO (or their nominee) will investigate and make the decision as to whether an escalation to the Information Commissioner's Office (ICO) is required.

Data incidents/breaches must be notified to the ICO within 72 hours, and must include details of the data subject and whether the breach might pose a high risk to their rights and freedoms.

Violations regarding record-keeping, security, breach notification, and privacy impact assessment obligations, can result in a penalty of up to €10 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 €20 million or 4% of global gross revenue.