DOCUMENT DETAILS

Document Name:	**Data breach management procedure**			
Approval body:	IT & MIS programme board			
Approval date:	March 2023			
Review date:	February 2025			
Document author	Data Protection Officer			
Document owner	Deputy CEO / CFO			
Applicability	Students	x	Staff	x
	Governors	x	Other	
Summary	The purpose of this document is to inform staff, governors and students what to do in the event of a data breach.			

DOCUMENT CONSULTATION & APPROVAL

Consultation person / body	**Date passed**
n/a	

Approval body	**Date approved**
Information Compliance Committee	9 May 2019
Information Compliance Committee (by circulation)	22 November 2019
Information Compliance Committee	8 June 2021
IT/MIS Board	02 March 2023

IMPACT ASSESSMENT

A significant negative impact has been identified in the following area and a full impact assessment / risk assessment is available.

Equality & diversity	No
UK GDPR	No
Health & safety	No
Safeguarding	No

Friendly version of policy available	No

POLICY CHANGES

Key updates	**Impact**	**Section reference**
References to UK GDPR changed to UK UK GDPR	none	throughout

CONTENTS

1. INTRODUCTION

1.1 Nottingham College holds and processes data consistent with the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR) (data protection legislation). As a data controller, the college must take all reasonable steps to process all personal data within the remit of the DPA and UK GDPR and all other legislative requirements. Suitable data security measures are taken by the college and its representatives to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach. Compromise of personal information, confidentiality, integrity or availability may result in harm to individuals, detrimental impact on service provision, reputational harm, legislative non-compliance, and/or fines under data protection legislation.

2. OBJECTIVE

2.1 This procedure sets out what to do in the event of a data breach (or suspected data breach). It ensures a consistent and effective approach is in place for managing data breach and information security incidents across the college.
2.2 This procedure relates to all personal data held by the college regardless of the format.

3. RESPONSIBILITIES

3.1 Although this procedure refers to employees throughout, it applies to staff and students, and includes temporary, casual or agency staff and contractors, consultants, suppliers and processors working for, or on behalf of the college.

4. POLICY STATEMENT

4.1 It is college policy to record all data breaches and deal with them in accordance with data protection legislation. This includes reporting any serious breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it and acting on any training or information security needs identified through logging and responding to breaches that do not reach the notification threshold.
4.2 Reporting of a data breach that represents a risk to the rights and freedoms of the data subject(s) is required by law and to not report a breach reaching the risk threshold is an offence. The ICO has the power to impose a financial penalty of up to €20m or 4% of annual turnover for breach of data protection legislation.

5. BREACH DEFINITION

4.1 A personal data breach is defined as a breach of security leading to the complete or partial destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This might include an event or action which compromises the confidentiality, integrity or availability of systems or personal data either accidentally or through deliberate act or lack of action or control.
4.2 A non-exhaustive list of potential incidents is shown below:

- Unauthorised use of, access to, or modification of personal data or information systems
- Unauthorised disclosure of personal data (either deliberate or through not following proper procedures and processes for the security of data)
- Improper sharing of data, or not taking appropriate steps to secure data when transmitting data within the organisation or to authorised agencies
- Loss or theft of confidential or sensitive data or equipment on which data is stored (e.g. USB drive, laptop, tablet, mobile phone)

- Attempts (successful or otherwise) to gain unauthorised access to information or IT systems
- Human error
- Unforeseen circumstances e.g. fire or flood – resulting in data loss
- 'Blagging' offences where information is obtained by deceit.

4.3 The college takes the following measures to mitigate any risk of data loss:

- Ensuring relevant training is undertaken by all staff
- The use of lockable cupboards (restricted access to keys)
- Restricted access to personal information files
- Setting up computer systems to allow restricted access to certain areas
- Password protected attachments, or secure links in Office 365, are used for the transmission of personal data sent by email
- Robust and reliable IT security features
- Data disposal is undertaken by accredited organisations and certified evidence provided
- Ensuring the use of confidential waste receptacles
- Ensuring robust data sharing agreements exist
- Ensuring access controls are relevant to staffing needs.

6. REPORTING AN INCIDENT

6.1 All staff are responsible for reporting a data breach or information security incident, or suspected incident. The incident must be reported as soon as possible to the Data Protection Officer. Incidents should also be reported by the individual to their line manager.

6.2 If an incident occurs outside of normal working hours, it should be reported as soon as is practicable. A breach report form is included in Appendix 1. Section 1 should be completed in order to report a breach and emailed to the DPO at dataprotectionofficer@nottinghamcollege.ac.uk.

7. CONTAINMENT AND RECOVERY

7.1 The Data Protection Officer (DPO) will first determine if a data breach has occurred and if so will, with the relevant colleagues, assess the level of risk it represents and establish the steps to be taken to stop the breach immediately and to minimise its effects.

7.2 If the breach is considered low risk, the DPO will log the incident and liaise with the colleague(s) who reported it to ensure accurate recording of the detail, and any necessary follow-up action, such as communication with data subject(s) affected and any staff training or communication need that might have been identified.

8. INVESTIGATION AND RISK ASSESSMENT

8.1 Where a breach is assessed as representing a risk, an investigation will be undertaken immediately. The potential adverse consequences for individuals will be assessed, as well as how serious or substantial the risks are, and how likely they are to occur. The impact on the college should also be assessed. The DPO, in collaboration with colleagues relevant to the nature of the breach, will support the investigation, which will usually occur at the point that the breach occurred.

8.2 Any investigation should take account of the following:

- The amount and sensitivity of data involved
- The current protection in place
- How the breach occurred (i.e. was data lost or stolen)
- Whether the data can be used by a third party and the potential or actual impact on data subjects

- Potential impact on the college, reputationally or financially
- To whom the breach might need reporting

9. NOTIFICATION

9.1 The DPO will determine who needs to be notified of the breach. A notifiable breach must be reported to the Information Commissioner's Office (ICO) within 72 hours of the college becoming aware of a breach.

9.2 Where it is necessary to inform the ICO of a breach, the college will provide all relevant facts of the breach and fully document the incident including measures and safeguards in place and how systems and controls were breached. The CEO and Principal and the Chair of Governors must be notified of any notification to the ICO.

9.3 Notification to the individuals whose personal data has been affected by an incident will include a description of how and when the breach occurred and the data that was involved. Individuals will be advised of actions that have been taken by the college to mitigate any risks. Individuals will be notified of how to contact the college for further information.

9.4 Consideration must be given to who should be notified based on the details of the incident. If potential illegal activity is known or is believed to have occurred or could occur as a result of the incident, then agencies such as the police, insurers, banks, and trade unions could also be notified.

9.5 The DPO, in discussion with the communications team and colleagues who are familiar with the facts of the breach, will determine what internal and external communication should take place.

9.6 All actions taken should be recorded in the data breach log.

10. EVALUATION AND RESPONSE

10.1 Once the initial incident is contained and any notifications made, the college will undertake a full review of the causes of the breach, the effectiveness of the response(s) to the breach, and whether any changes to systems, policies and procedures are required.

10.2 This may include:

- Where personal data is held and how it is stored
- Current identified risks, and potential weaknesses with current measures
- Transmission and transfer of data methods
- Staff awareness
- The evaluation and response process

10.3 Existing controls including data protection impact assessments will be reviewed to determine their adequacy and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

11. RECORDS

10.1 The DPO keeps a log of all data breaches, and any relevant allied documentation.

12. REFERENCES

12.1 The college policies and guidelines which should be reviewed in conjunction with this policy include:

- Nottingham College Data Protection Policy
- Business Continuity Policy and associated incident management plans
- Information Security Policy
- Social Media Guidelines

- Freedom of Information Policy
- Information Security Policy
- Data Retention and Disposal Policy
- Disciplinary Policy
- Safeguarding Policy

12.2 Relevant legislation includes:

- The Regulation of Investigatory Powers Act 2000;
- The Telecommunications (Lawful Business Practice), (Interception of Communications) Regulations 2000;
- The Communications Act 2003;
- Data Protection Act 2018/UK General Data Protection Regulation;
- The Human Rights Act 1998;
- The Equality Act 2010;
- Freedom of Information Act 2000

13. APPENDICES

Appendix 1: Data Breach Report Form

APPENDIX 1: Data Breach Report Form

Please act promptly to report any data breaches. If you discover a data breach, please notify the Data Protection Officer on dataprotectionofficer@nottinghamcollege.ac.uk, or on 07976 224463 and your line manager. If the breach is non-urgent, please use the form below to report it and email it to the Data Protection Officer.

Section 1: Notification of Data Security Breach	To be completed by person reporting incident with Head of Department/Faculty
Date incident was discovered:	
Date(s) and location of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	

For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by the Investigating Officer in consultation with the Head of Department/Faculty affected by the breach
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost	
Is the information unique? Will its loss have adverse operational, financial legal, liability or reputational consequences for the college or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories: 1. **HIGH RISK** personal data (as defined in the Data Protection Act/ UK GDPR) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) criminal offence/conviction and/or related data	

2. Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas; 3. Personal information relating to vulnerable adults and children; 4. Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed; 5. Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals. 6. Security information that would compromise the safety of individuals if disclosed.	

Section 3: Action taken	To be completed by Data Protection Officer and/or Investigating Officer
Incident number	e.g. year/001
Action taken by responsible officer/s:	
Was incident reported to Police?	Yes/No If YES, notified on (date):
Follow up action required/recommended:	

For use of Data Protection Officer and/or Investigating Officer:	
Notification to ICO	YES/NO If YES, notified on: Details:
Notification to data subjects	YES/NO If YES, notified on: Details:
Notification to other external, regulator/stakeholder	YES/NO If YES, notified on: Details: