DOCUMENT DETAILS

Document Name:	Nottingham College Data Breach Management Procedure
Document reference	IT/MAP/180418
Version	1.1
Issue Date:	April 2018
Review Date:	October 2018
Document Author	Michael Davies
Document Owner	Jo Clifford
Applicability	All staff, volunteers and Governors of Nottingham College, all other parties under contract
Summary	The purpose of this document is to set out the policy and procedure for Data Breach Management

DOCUMENT CONTROL

Version history			
Version	Date	Reason for release/version update	Issued by
1	25 January 2018	First draft	Michael Davies
1.1	8 March 2018	Update following feedback from CEO	Michael Davies

DOCUMENT APPROVAL

Approving person/body	Job Role (where applicable)	Date Approved

CONTENTS

1. INTRODUCTION

Nottingham College holds and processes data consistent with the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR) legislation. As a Data Controller, the College must take all reasonable steps to process all personal data within the remit of the DPA and 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 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 DPA or GDPR.

2. OBJECTIVE

The purpose of this procedure is to provide a framework for the containment of a data breach, to minimise risk, identify appropriate reporting mechanisms, and the identification of action(s) required to secure personal data and prevent any further breach.

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.

This procedure relates to all personal and sensitive data held by the College regardless of the format. 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.
The scope of this procedure includes all data security breaches including both confirmed, or suspected.

3. POLICY AND LEGISLATIVE CONNECTIONS

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

- Data Protection Policy
- General Data Protection Regulation (GDPR) Policy
- Social Media Policy
- Freedom of Information Policy
- Information Security Policy
- Archiving Policy
- Disciplinary Policy
- Safeguarding Policy

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 1998/General Data Protection Regulation;
- The Human Rights Act 1998;
- The Defamation Act 1996 and the Equality Act 2010;
- Malicious Communications Act 1988;
- Computer Misuse Act 1990;
- Freedom of Information Act 2000,
- Road Traffic Act 1988

4. BREACH DEFINITION

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 or sensitive data (as defined in the Data Protection Act and General Data Protection Regulation. 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.

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 or sensitive 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 pen 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
- Hacking attack
- 'Blagging' offences where information is obtained by deceit.

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

- Implements robust policies and procedures
- Ensures relevant training is undertaken by all staff
- The use of lockable cupboards (restricted access to keys)
- Password protection on personal information files

- Setting up computer systems to allow restricted access to certain areas
- Not allowing personal data to be taken off site (as hard copy, on laptop or on memory stick) without adequate safeguarding e.g. encryption
- Where personal data can be taken off site, instruction are provided on safe keeping
- Appropriate security data backup procedures are implemented and tested.
- Password protected attachments are used for the transmission of personal data sent by email
- Robust and reliable IT security features
- Robust secure on site IT storage facility
- Data disposal is undertaken by accredited organisations and certified evidence provided.
- Ensure the use of confidential waste receptacles
- Ensure robust data sharing agreements exist
- Ensure access controls are relevant to staffing needs and re assess where required
- Measures to ensure safe transfers of data outside of the EU/EEU where cross border sharing is necessary

5. REPORTING AN INCIDENT

All staff are responsible for reporting a data breach or information security incident, or suspected incident. The incident must be reported immediately it is known or suspected to the person identified as holding the responsibilities of the Data Protection Officer. Incidents should also be reported by the individual to their line management or supervisor.

If an incident occurs outside of normal working hours, it should be reported as soon as is practicable.

An incident report must be completed by the individual who reports the incident. An incident report form is included in Appendix 1.

6. CONTAINMENT AND RECOVERY

The Data Protection Officer (DPO) will first determine if a data breach has occurred and if the breach is still occurring. If a breach has occurred and is still occurring, then the appropriate steps will be taken to stop the breach immediately and to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison with any relevant resources to establish the severity of the breach, assess the risk, and to determine who will take the lead in investigating the breach. This will depend on the nature of the breach. Reference may be made to the Disciplinary Policy if required.

An Investigating Officer (IO) will be appointed and will determine what can be done to contain the breach. The IO will establish who needs to be notified as part of the initial containment,

informing relevant authorities which may include the police, supervisory authorities, and individuals depending on the severity of the breach and the level of risk to individuals.

The IO will work with relevant resources to determine the course of action to be taken to ensure a resolution to the incident

7. INVESTIGATION AND RISK ASSESSMENT

An investigation will be undertaken by the IO immediately (supported by the DPO and other resources) and wherever possible within 24 hours of the breach being discovered/reported.

The IO will investigate the breach and assess the risk associated with it. This will include the potential adverse consequences for individuals, how serious or substantial the risks are, and how likely they are to occur. The impact on the College should also be assessed.

The investigation should take account of the following:

- The type of data involved
- The sensitivity of the data
- The current protection in place
- How did the breach occur (e.g. was data lost or stolen)?
- How could the data be used by a third party (illegal or inappropriate use)?
- Who is affected, numbers involved, potential effects on these data subjects
- Impact on the College
- Wider consequences to the breach under GDPR
- Who to inform

8. NOTIFICATION

The IO and/or the DPO and the Vice Principal – Finance, 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.

Every incident should be assessed individually, but the following should be considered as part of the decision to notify:

- Whether there are any legal/contractual obligations to notify
- Whether notification would assist the affected individuals to mitigate their risks
- Whether notification would prevent further unlawful use of data
- Who needs to be notified
- How will notification help to protect the College?
- What details will be released in the notification

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 College Chief Executive Officer and the Chair of Governors must be notified in advance of the notification to the ICO.

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.

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.

The IO and/or the DPO and the Vice Principal – Finance in discussion with the Communications team will determine what internal and external communications should take place.

All actions taken should be recorded in the log of the incident.

9. EVALUATION AND RESPONSE

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.

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

Existing controls including privacy 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.

10. APPENDICES

Appendix 1: Data Breach Report Form

APPENDIX 1: Data Breach Report Form
DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify the Data Protection Officer and your line manager/supervisor.

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) of incident:	
Place 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:	
HIGH RISK personal data □ (as defined in the Data Protection Act/ 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	

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;	
Personal information relating to vulnerable adults and children;	
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;	
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
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: