Data Breach Policy and Procedures

Author	Executive Director of Facilities and Resources
Date	July 2022
Person Responsible	Risk Manager and DPO
Approval/ review bodies	SLT
Frequency of Review*	36 months

Policies will be reviewed more frequently if legal changes or good practice require

Review History:		
Date of review	Reviewed by	Reason for review
September 2018	Executive Director of Facilities and Resources Data Protection Officer	Authored Reviewed
July 2022	Risk Manager	Routine review

Contents

Related policies and procedures:

1. Data Protection Policy
2. Freedom of Information Policy
3. IT Conditions of Use Policy
4. Dealing with Malicious Communication Procedure
5. Mobile Device and Communications Policy
6. Staff Code of Conduct
7. Staff Disciplinary policy and procedure (Conduct**)**

1. Introduction

1.1. North Kent College ("the College") collects, holds, processes and shares personal data, a valuable asset that needs to be suitably protected.

1.2. All reasonable care is taken by the College to protect personal data to avoid a data protection breach (either accidental or deliberate) that could compromise data security.

1.3. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance and/or financial costs.

2. Purpose and Scope

2.1. The College is obliged under UK Data Protection legislation[1] to have in place an institutional framework which ensures the security of all personal data during its lifecycle and which includes clear lines of responsibility.

2.2. This document sets out the procedure to be followed to ensure a consistent and effective approach is taken when managing data breach and information security incidents across the College.

2.3. This procedure relates to all personal and special categories (sensitive) data held and/or processed by the College, regardless of format. For clarity, this includes "hard copy" formats.

2.4. This procedure applies to all staff and students at the College. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the College.

2.5. The objective of this procedure is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

3. Definitions/Types of breach

3.1. For the purpose of this procedure, data security breaches include both confirmed and suspected incidents.

3.2. An incident in the context of this procedure is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the College's information assets and/or reputation.

[1] UK Data Protection Act 2018 and UK General Data Protection Regulation

3.3. An incident includes, but is not restricted to, the following:

3.3.1. loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/ tablet device, or paper record);

3.3.2. equipment theft or failure (which could potentially compromise data security);

3.3.3. loss of data though system security failure;

3.3.4. unauthorised use of, access to or modification of data or information systems;

3.3.5. attempts (failed or successful) to gain unauthorised access to information or IT system(s);

3.3.6. unauthorised disclosure of sensitive/confidential data (whether accidental or deliberate);

3.3.7. website defacement;

3.3.8. hacking attack;

3.3.9. unforeseen circumstances such as a fire or flood with the potential to compromise data security or cause loss of data;

3.3.10. human error, where such error has the potential to compromise data security; and/or

3.3.11. “blagging” offences where information is obtained by deceiving the organisation who holds it, or individuals who have access to it.

4. Reporting an incident

4.1. Any individual who accesses, uses or manages the College’s information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer who will appoint the appropriate staff to investigate.

4.2. If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

4.3. The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (refer to Appendix 1).

4.4. All staff should be aware that any breach of Data Protection legislation may result in the College’s Disciplinary Procedures being instigated.

5. Containment and recovery

5.1. The Data Protection Officer ('DPO') will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately, aiming to minimise the effect of the breach.

5.2. An initial assessment will be made by the DPO in liaison with relevant staff to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (this will depend on the nature of the breach; in some cases, it could be the DPO).

5.3. The Lead Investigation Officer ('LIO') will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

5.4. The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

5.5. Advice from experts across the College may be sought in resolving the incident promptly.

5.6. The LIO, in liaison with the relevant staff will determine the suitable course of action to be taken to ensure a resolution to the incident.

6. Investigation and risk assessment

6.1. An investigation will be undertaken by the LIO immediately and, wherever possible, within 24 hours of the breach being discovered/ reported.

6.2. The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

6.3. The investigation will need to take into account the following:

6.3.1. the type of data involved;

6.3.2. its sensitivity;

6.3.3. the protections that are in place (e.g. encryptions);

6.3.4. what has happened to the data (e.g. has it been lost or stolen);

6.3.5. whether the data could be put to any illegal or inappropriate use;

6.3.6. data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s); and

6.3.7. whether there are wider consequences relating to the breach.

The LIO will keep the DPO informed at every step of the investigation.

7. Notification

7.1. The DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office ("ICO") will need to be notified of the breach and, if so, notify them within 72 hours of becoming aware of the breach, where feasible.

7.2. Every incident will be assessed on a case-by-case basis; however, the following will need to be considered:

7.2.1. whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under UK Data Protection legislation[2];

7.2.2. whether notifying affected Data Subjects would assist them (e.g. could they act on the information to mitigate risks?);

7.2.3. whether notification would help prevent the unauthorised or unlawful use of personal data;

7.2.4. whether there are any legal/contractual notification requirements; and

7.2.5. the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

7.3. Individuals whose personal data has been affected by the incident and, where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the College for further information or to ask questions on what has occurred.

7.4. The LIO and/or the DPO must consider notifying third parties such as the police, insurers, banks or credit card companies and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

7.5. The LIO and/or the DPO will consider whether the Marketing Department should be informed regarding a press release and being ready to handle any incoming press enquiries.

[2] Individual Rights under the UK Data Protection Act 2018:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

7.6. A record will be kept of any personal data breach, regardless of whether notification was required.

8. Evaluation and response

8.1. Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

8.2. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

8.3. The review will consider:

8.3.1. where and how personal data is held and where and how it is stored;

8.3.2. where the biggest risks lie including identifying potential weak points within existing security measures;

8.3.3. whether methods of transmission are secure; sharing minimum amount of data necessary; and

8.3.4. staff awareness.

8.4. If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Senior Leadership Team.

Appendix 1: Data Breach Report Form

Please act promptly to report any data breaches. If you discover, or suspect, a data breach, please notify your Line Manager and the Data Protection Officer promptly. Where possible, do this by phone, then complete **Section 1** of this form and e-mail it to the Data Protection Officer (DPO@northkent.ac.uk) and cc your Line Manager.

Section 1: **Notification of Data Security Breach**	**To be completed by person discovering data breach / potential breach**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (e-mail address, telephone number):	
Brief description of incident or details of the information lost / potentially 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 Lead Investigation Officer in consultation with the Manager of area affected by the breach and if appropriate IT where applicable**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss / potential loss:	
What is the nature of the information lost / potentially lost?	
How much data has been lost / could have been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
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	
• Special categories personal data (as defined in the Data Protection Legislation) relating to a living, identifiable individual/s	
a) racial or ethnic origin;	
b) political opinions or religious beliefs;	
c) trade union membership;	
d) genetics;	
e) biometrics (where used for ID purposes)	
f) health;	
g) sex life or sexual orientation	

Section 2: **Assessment of Severity**	**To be completed by the Lead Investigation Officer in consultation with the Manager of area affected by the breach and if appropriate IT where applicable**
• 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.	
Data Protection Officer and/or Lead Investigation Officer to consider whether it should be escalated to the appropriate SLT.	

Section 3: Action taken	To be completed by Data Protection Officer and/or Lead Investigation Officer
Incident number in the format: DB-year-001 (number to be provided by DPO)	
Report received by:	
On (date):	
Action taken by responsible Manager / staff:	
Was incident reported to Police? **Yes/No**	
If YES: notified on (date):	
Crime Reference Number:	
Follow up action required / recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer and / or Lead Officer:	
Notification to ICO **YES/NO**	
If YES, notified on:	
Details (also attach copy of notification sent):	
Notification to data subjects **YES/NO**	
If YES, notified on:	
Details (also attach copy of notification sent):	
Notification to other external, regulator/ stakeholder **YES/NO**	
If YES, notified on:	
Details (also attach copy of notification sent):	