

BREACH OF DATA POLICY

1. Purpose

This policy establishes the Newbattle Abbey College guidelines for how to deal with a personal data breach under the GDPR.

2. Scope

The General Data Protection Regulation (GDPR) introduces mandatory obligations on organisations, which process and exercise control over personal data (known as "controllers") to notify personal data breaches to the relevant supervisory authority, which is the Information Commissioner's Office (ICO) for the UK, and in some cases to the individual data subjects themselves. The College is a controller, and subject to these mandatory obligations.

This policy relates to all personal and any special categories (sensitive) data held by the College regardless of format.

This policy 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.

This policy should therefore be made available to all people in the above categories.

The aim of this policy is to ensure that data breaches are dealt with effectively and the College complies with its GDPR obligations. Adhering to this policy will ensure that:

- incidents are reported swiftly and can be properly investigated
- incidents are dealt with in a timely manner and normal operations restored
- incidents are recorded and documented
- the impact of the incident is understood, and action is taken to prevent further damage
- the ICO and data subjects are informed as required in more serious cases
- incidents are reviewed, and lessons learned

3. Types of Breach

The GDPR defines a data breach as *“a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.”*

Data security breaches include both confirmed and non-confirmed breaches.

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

- 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)
- equipment theft or failure
- system failure
- unauthorised use of, access to or modification of data or information systems
- attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- unauthorised disclosure of sensitive/confidential data
- website defacement
- hacking attack
- unforeseen circumstances such as a fire or flood
- human error
- 'blagging' offences where information is obtained by deceiving the organisation who holds it

In any situation where staff are uncertain whether an incident constitutes a breach of security, they consult the Director of Operations **without delay**. If there are IT issues, such as the security of the network being compromised, the college IT Services & Digital Support Officer should also be informed immediately.

4. Breach Record

The GDPR requires that information related to a breach should be retained which shall include:

- documentation on data breaches
- their nature
- remedial action taken

Please refer to section 5 for more detail on what documents and correspondence should be kept in relation to a breach.

5. Procedure

5.1 Discovery of Breach

Any individual who accesses, uses or manages information on behalf of the college is responsible for reporting any data breach and information security incidents immediately to DPO@nac.ac.uk. This mailbox is monitored by the Director of Operations and the Senior Administrator. The individual should also report the breach to their line manager.

The Director of Operations or the Senior Administrator will immediately consult the Data Protection Officer who will coordinate the situation going forward.

If the breach occurs or is discovered outside normal working hours, it must be reported immediately to DPO@nac.ac.uk, and if possible, communicated to their line manager and/or the Director of Operations.

After the member of staff has notified relevant personnel of the breach, they should complete a Breach Report Form, found at Appendix 1. 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. The report shall form the basis of the college's obligation to keep records of all breaches or potential breaches and shall be filed securely in an electronic folder accessible only by members of the Senior Management Team.

All correspondence and other documentation should be retained and become part of the Breach Record.

Please note that the above actions are critical as the 72-hour period to notify the ICO begins as soon as the person discovers the breach or potential breach

5.2 Containment and Recovery

Once the relevant personnel have been made aware of the breach, they will take the following steps:

1. Identifying who needs to be aware of the breach and informing them of how they need to assist.
2. Identifying and implementing how to contain the breach eg changing passwords, remotely wiping a device etc.
3. Determining whether police/insurance/banks/trade unions/credit card companies should be informed of the breach.
4. Determining whether the breach should be notified to the ICO or any other regulatory body, or whether it should be notified to the data subject.

All actions and documentation should become part of the Breach Record.

5.3 Risk Assessment

An initial investigation will be undertaken immediately, with the knowledge that there is a 72-hour breach notification requirement to the ICO. The relevant personnel 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. The investigation will need to take account of:

- the type of data involved
- its sensitivity
- the protections that are in place (e.g. encryptions)
- what has happened to the data (e.g. has it been lost or stolen)

- whether the data could be put to any illegal or inappropriate use
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach

A risk assessment form, found at Appendix 2, should be completed and become part of the Breach Record.

5.4 Notification

5.4.1 The ICO must be notified of any personal data breach where it is likely to result in a risk to the rights and freedoms of individuals.

Where required, the ICO must be notified without undue delay and in any case within 72 hours of the breach. This period commences immediately upon receipt of notification of a breach by the relevant personnel and recognition that a breach has indeed occurred. There are no exceptions to the 72 hours, and this will include eg weekends and public holidays.

A report to the ICO must include the nature of the breach, categories of data, number of data records, number of people affected, name and contact details of DPO, likely consequences of the breach and action taken.

5.4.2 The individual data subject must be notified where there is a **high risk** to the rights and freedoms of individuals.

Where required, the data subject must be informed **without undue delay**. There is no overall deadline for this, but communications should be made as early as possible and in co-operation with the ICO.

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.

All correspondence and documentation should become part of the Breach Record.

5.5 Evaluation

Once the initial incident is contained, the relevant personnel 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.

The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

A review and actions taken form, found at Appendix 3, should become part of the Breach Record.

6. Disciplinary

Failure to comply with these guidelines will result in sanctions ranging from disciplinary procedures such as verbal and written warnings, through to dismissal.

7. Appendices

Appendix 1: Personal Data Breach Record Form

Appendix 2: Personal Data Breach Risk Assessment Form

Appendix 3: Personal Data Breach Evaluation Form

This Policy should be read in conjunction with other relevant College policies, procedures and guidance documents, whether specifically listed above or subsequently published or amended.

The College reserves the right to update, introduce, or revise policies and procedures from time to time.

Compliance with the most current versions of applicable policies and procedures, as published, is expected.

Title:	Breach of Data Policy
Lead Officer:	DPO
Date last reviewed	February 2025
Next Review date:	February 2028
Approved By:	Audit & Risk Committee
Date first approved:	January 2020

APPENDIX 1
Personal Data Breach Record Form

To be completed by the member of staff who becomes/is made aware of a personal data breach	
Name	
Department	
Date and time breach occurred	
When and where did the breach occur?	
Director of Operations notified? Y/N	
Date, time and method of notification	
What type of personal data breach has occurred?	
Personal data has been accidentally lost or deleted by an employee.	
Personal data has been corrupted.	
Someone accesses personal data or passes it on without proper authorisation.	

A network intrusion by a third party (e.g. a hacking incident or another type of cyber security attack).	
Data or equipment on which personal data is stored has been lost or stolen.	
Inadequate security controls (such as weak passwords) result in an authorised person gaining access to an IT system which includes personal data.	
Human error resulting in information being sent to the incorrect recipient.	
Personal data is destroyed by unforeseen circumstances such as fire or flood.	
'Blagging' offences where information is obtained by deceiving the organisation who holds it.	
Other (please specify)	
What type of personal data is involved?	
Is any confidential or special category data involved in the breach e.g. medical/health information, financial information or personnel data? If so what?	
What is the approximate number of individuals whose personal data are involved in the breach?	

Details of any individuals or organisations involved in the breach
Details of individuals or organisations who are aware of the breach, including details of when and how they became aware.

APPENDIX 2

Personal Data Breach Risk Assessment Form

What type of data is involved?	
Did the data include special category data (formerly sensitive personal data) e.g. health information?	
Did the data include data that was confidential, or which could be used to commit fraud or identity theft (eg bank details)?	

What could the data tell a third party about the individual?	
When did the personal data breach occur?	
What was the time lag between the personal data breach occurring and the discovery of the personal data breach?	
If data has been lost or stolen, are there any protections in place such as encryption?	
If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relates?	
The measures taken or proposed to be taken to address the personal data breach, including any measures to mitigate its possible adverse effects.	

Assessment of whether the personal data breach should be notified to the ICO.	
Assessment of whether the personal data breach should be notified to individual data subjects.	

APPENDIX 3
PERSONAL DATA BREACH EVALUATION FORM

Part 2 - For completion by Director of Operations or other senior manager

The potential effect of the breach (e.g. potential loss of personal data, however laptop reported lost immediately, password protected and data encrypted, hard drive can be wiped remotely – effect of personal data breach minimal)

The potential cause of the breach

Confirmation of any remedial action taken (e.g. hard drive wiped remotely within 6 hours of laptop reported as lost)