DATA BREACH POLICY & PROCEDURE

1.0 Introduction

1.1 West Nottinghamshire College holds, processes, and shares a large amount of personal data, a valuable asset that needs to be suitably protected.

1.2 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise 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 noncompliance, and/or fines under GDPR.

2.0 Purpose

2.1 WNC is obliged under the Data Protection Act and the General Data Protection Regulations to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the College.

3.0 Scope

3.1 This policy relates to all personal and sensitive data held by the College regardless of format.

3.2 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.

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

4.0 Definition / Types of Breach

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

4.2 A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

An incident in the context of this policy 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.

4.3 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.
- 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.
- Hacking attack.
- Unforeseen circumstances such as a fire or flood resulting in data loss.
- Human error.
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

5.0 Reporting an incident

5.1 Any individual who accesses, uses or manages the College's information is responsible for reporting data breach and information security incidents immediately to dataprotection@wnc.ac.uk.

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

5.3 The report will 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. See Appendix 1.

6.0 Containment and Recovery

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

6.2 An initial assessment will be made by the DPO in liaison with relevant officers to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach in some cases it could be the DPO).

6.3 The Investigating Officer (IO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

6.4 The IO will establish who may need to be notified as part of the initial containment and will inform the police, supervisory authorities and individuals depending on the level of risk to the rights and freedoms of individuals.

6.5 The IO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

7.0 Investigation and Risk Assessment

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

7.2 The IO 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.

7.3 The investigation will need to take into account the following:

- the type of data involved.
- its sensitivity.
- the protections are in place (e.g. encryption).
- what's happened to the data, has it been lost or stolen.
- whether the data could be put to any illegal or inappropriate use.
- who the individuals are, number of individuals involved and the potential effects on those data subject(s).
- whether there are wider consequences to the breach under the GDPR.

8.0 Notification

8.1 The IO and / or the DPO, Director of IT and the Deputy Principal, will determine who needs to be notified of the breach.

8.2 The College is required to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

8.3 A notifiable breach must be reported to the ICO within 72 hours of the College becoming aware of it.

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

- Whether there are any legal/contractual notification requirements.

- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?
- Where there is likely to be a risk to the freedom of individuals Information Commissioner's Office (ICO) should be notified.

8.3 Notification to the individuals whose personal data has been affected by the incident 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.

8.4 The IO and or the DPO must consider notifying third parties such as the police, insurers, bank 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.

8.5 The IO and or the DPO will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

8.6 All actions will be recorded by the DPO.

9.0 Evaluation and response

9.1 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.

9.2 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.

9.3 The review will consider:

- Where and how personal data is held and where and how it is stored.
- Where the biggest risks lie and will identify any further potential weak points within its existing measures.
- Whether methods of transmission are secure; sharing minimum amount of data necessary.
- Identifying weak points within existing security measures.
- Staff awareness.
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

9.4 If deemed necessary a report recommending any changes to systems, policies and procedures will be considered.

APPENDIX 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify your Head of Department/Service immediately, complete this form and email it to Head of IT & Learning Resources and Director: IT, Estates & Learning Resources (owen.williams@wnc.ac.uk and gavin.peake@wnc.ac.uk).

West Nottinghamshire College **Root Cause Analysis (RCA)**	
RCA ID:	[CLIENTNAME - BREACH_ID- BREACH TITLE]
Date:	
Issue:	
Issue Description:	
Customer Impact:	
Sequence of Events:	
Communication Process Used:	
Root Cause:	[E.g. Human mistake happened during the upload of the Apprentice form onto One File.]
Corrective Actions:	
1.1 Preventative Action 1	
1.2 Action Owner	
1.3 Target Date	
1.4 Actual Completion Date	
1.5 Success Criteria	
1.6 Supporting Doc (if required)	
RCA Owner (s):	
RCA Reviewer:	
RCA Requestor:	
Sign-off and record outcomes	
Measures approved by:	[name/date]
DPO advice / Sign off	