Northern College

Data Protection and Information Security Policy

Who does the policy apply to?	This policy applies to: • all employees of the College; • members of the Board of Governors and other committee members; • sessional and agency staff working for the College; • any other third parties who work on delivering College services and are paid through a contract for services.
Aims	The policy aims to ensure that the College: • complies with data protection and freedom of information legislation, and relevant codes of practice issued by the Information Commissioner; • maintains robust and effective information security; • upholds the rights of data subjects regarding the processing of their personal data.
To be read in conjunction with	• Data Breach Protocol; • Privacy Notices; • A Guide to Your Rights – Personal Data; • Data Retention Policy; • Model Contract Terms - Data Protection; • Data Protection Impact Assessment Procedure; • CCTV Code of Practice; • ICT Acceptable Use Policy; • ICT Security Procedures. Relevant legislation: • the UK-General Data Protection Regulation (GDPR) • the Data Protection Act 2018 • the Privacy and Electronic Communications (PECR) Regulations 2003 • The Freedom of Information Act 2000 • The Environmental Information Regulations 2004
Further advice may be sought from	Data Protection Officer Head of MIS and ICT
Review arrangements	This policy will be reviewed every three years to ensure its continuing relevance and effectiveness. The College may review the policy prior to this date should operational and/or legislative/guidance matters require it.

	Further details regarding revisions, the consultation and approval process and review cycle can be found at paragraph 6.

1. Policy Statement

1.1. In order to deliver its mission to provide outstanding adult residential and community education the College needs to collect, use and store personal data about a range of individuals including its employees, suppliers, students, governors, and visitors.

1.2. The College is committed to complying with data protection and freedom of information legislation, and maintaining robust information security.

1.3. The College will take all reasonable steps to ensure that its processing of personal data is fair, lawful, and compliant with data protection legislation, and that all the information it processes is held securely.

2. Scope

2.1. The policy applies to all personal data stored either electronically or in paper form, including any systems or data attached to the College's computer or telephone networks, any systems supplied by the College, any communications sent to or from the College, and any data which is owned by the College and held on systems external to the College's network.

3. Data Protection Principles

3.1. When using personal data the College will comply with data protection laws by ensuring that personal data is:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- accurate and kept up to date, meaning that every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified as soon as possible;
- kept for no longer than is necessary for the purposes for which it is being processed; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Policy Details

4.1. In order to achieve this the College will:

- put in place appropriate policies and procedures to ensure compliance with relevant legislation;
- appoint a Data Protection Officer (DPO) and ensure that the DPO is able to carry out the tasks specified in the UK-GDPR;
- maintain appropriate records of its processing activities;
- report and investigate actual or suspected breaches of information security and take appropriate corrective action;
- notify the Information Commissioner and data subjects of data security breaches in line with legal requirements and guidance from the ICO;
- cooperate fully with the ICO when requested to do so;

- take appropriate measures to ensure that the rights of data subjects are upheld;
- carry out privacy impact assessments where appropriate;
- ensure that any data processors it engages provide sufficient guarantees of compliance and enter into an appropriate written contract;
- ensure compliance with the Freedom of Information Act and the Environmental Information Regulations;
- ensure CCTV systems are operated in accordance with legislation, guidance and good practice;
- use a combination of internal and external audit to assure compliance against standards and best practice, including against internal policies and procedures;
- ensure that information security risks are identified, assessed, and managed;
- implement appropriate technical, physical and organisational measures and procedures for ensuring the security of personal data appropriate to the risk;
- maintain network security controls to ensure the protection of information within its networks;
- provide tools and guidance to ensure the secure transfer of information both within its networks and with external entities, in line with the classification and handling requirements associated with that information;
- ensure the correct and secure operations of information processing systems including documented operating procedures, controls against malware and vulnerability management;
- have in place arrangements to protect critical business processes from the effects of major failures of information systems and to ensure their timely recovery in line with documented business needs, including appropriate backup routines and built-in resilience;
- provide relevant training and development for staff and governors, appropriate to their role.

5. Roles and Responsibilities

The Board of Governors will:

5.1. assume overall accountability for information governance and security;

5.2. challenge and hold the College's management to account for ensuring effective information governance and security arrangements are in place.

The Executive Leadership Team (ELT) will:

5.3. have overall responsibility for information as a strategic College asset, ensuring that the value of information to the College is understood and recognised and that measures are in place to protect against risk;

5.4. lead and champion information governance and security across the College;

5.5. foster a culture that values, protects and uses information for the success of the College and the benefit of our stakeholders;

5.6. put in place and resource an appropriate structure for the effective oversight of information governance and security;

5.7. approve any new data sets or processes which involve the use of personal data, ensuring that they are in line with data protection legislation and College policies.

The Risk Management and Business Continuity Group will:

5.8. have cross-College oversight of information governance and security;

5.9. advise the ELT on information processing, security, risks and controls;

5.10. develop and maintain information governance policies, procedures and guidance.

Data Protection Officer (DPO)

5.11. The role of the Data Protection Officer is set out in Articles 37-39 of the UK-General Data Protection Regulation and can be summarised as follows:

- to inform and advise the College and College staff of their data protection obligations;
- to act in the interests of data subjects in providing advice and guidance to the College in information governance compliance;
- to monitor the College's compliance with data protection legislation;
- to provide advice where required on data protection privacy impact assessments;
- to cooperate with and be the point of contact for the ICO.

5.12. In addition the DPO will also:
- coordinate requests for information (SARs, FOI requests, EIR requests);
- carry out data protection audits and provide recommendations to strengthen controls;
- oversee the effective handling of any complaints relating to information governance.

Members of the College Leadership Team (CLT) will:

5.13. lead and champion information governance in their team;
5.14. ensure that the processing of personal data in their team is compliant with data protection legislation;
5.15. put into place appropriate procedures in their team;
5.16. assess, monitor and manage information governance risks in their team;
5.17. ensure that staff within their team have undertaken appropriate data protection and information security training and are aware of relevant policies, procedures, and guidance;
5.18. ensure that appropriate technical and organisational measures are in place within their team to protect personal data;
5.19. maintain an information asset register for their team.

The Head of MIS and ICT will:

5.20. oversee the management of information security;
5.21. determine and implement the appropriate level of security controls that should be applied to information systems;
5.22. provide specialist advice on information security;
5.23. oversee ICT data security incidents;
5.24. establish and oversee the implementation of appropriate controls, processes and procedures for information security;
5.25. oversee access to systems driven by business needs, including a formal user registration and de-registration procedure and mandatory authentication methods.

All staff will:

5.26. comply with data protection legislation;
5.27. adhere to related College policies and procedures;
5.28. ensure that they are familiar with related guidance;
5.29. undertake data protection training and information security appropriate to their role;
5.30. report data security incidents immediately in accordance with reporting procedures;
5.31. ensure that data is shared appropriately and securely;
5.32. ensure that data is deleted/destroyed in a secure manner when no longer required;
5.33. process personal data in accordance with the rights of data subjects and assist with the collation of information for Subject Access Requests (SARs);
5.34. assist in the completion and maintenance of information asset registers and records retention schedules;
5.35. raise concerns with their line manager or the Data Protection Officer in a timely manner;
5.36. assist with responses to requests for information made under the Freedom of Information Act and the Environmental Information Regulations;

5.37. ensure that they keep confidential and secure all personal data that they collect, store, use and come into contact with during the performance of their duties;

5.38. not release or disclose any personal data outside the College, or inside the College to College personnel not authorised to access it, without specific authorisation from their manager or the Data Protection Officer.

6. Policy sign off and ownership details

Document Name:	Data Protection and Information Security
Version Number:	1.0
Effective from:	15 July 2022
Next scheduled review date:	July 2025
Policy owner:	Data Protection Officer
Approved by:	The Board of Governors

7. 9. Revision history

Version No	Effective date	Revision description/summary of changes	Author
1.0	15 July 2022	Complete re-write to combine data protection and information security into a single policy.	Data Protection Officer (Sarah Johnson)