NEWBATTLE ABBEY COLLEGE

INFORMATION SECURITY POLICY

1 Purpose and Scope

1.1 The Information Security Policy (the "Policy") sets out Newbattle Abbey College's (the "College") approach to information security risk management. The Policy is in place to support the strategic vision of the College and to facilitate the protection of the College's information assets and technology services against compromise of their confidentiality, integrity, or availability. Whilst doing this, it recognises the ability to discover, develop and share knowledge must be maintained.

1.2 The Policy advocates our approach to information security risk management that is achieved by identifying and assessing information security threats and developing and implementing a combination of people, process, and technology controls to mitigate against them where possible. This Policy is managed and developed by the Business & Resources Manager on behalf of the College.

1.3 The Policy applies to:

- Everyone within Newbattle Abbey College who accesses College information assets or technology, from any location and by whatever means. This includes users, students, and alumni. **Users are defined as all staff, contractors, visitors, consultants and any third parties engaged to support College activity and who have any authorised access to any College information**.
- Technologies or services used to access or process College information assets.
- Information assets processed in relation to any College function, including by, for, on behalf of, or with, external parties.
- Information assets that are stored by the College or an external service provider on behalf of the College.
- Information that is created or transferred from and/or to the College for any functional purpose.
- 3rd party, public, civic or other information that the College is storing, curating or using on behalf of any other party.
- Internal and/or external processes that are used to process, transfer or store College information.

2 Objectives

2.1 The policy is designed to:

- Protect the College’s information assets and technology against compromise of confidentiality, integrity (including non-repudiation) and availability. Non-repudiation implies that in a transaction one party cannot deny having received a transaction nor can the other party deny having initiated it. It is often included within integrity but is expanded here for completeness.
- Support the College’s strategic vision through an approach which effectively balances usability and security.
- Facilitate a ‘security aware’ culture across the College and promote Information Security as everyone’s responsibility.
- Protect the College’s own information assets, 3rd party data assets being processed or held by the College on behalf of another party and the associated technology by identifying, managing and mitigating information security threats and risks.
- Define security requirements that are effective, sustainable, and measurable.
- Assist in the compliance of contractual, legal, or regulatory obligations.
- Identify, contain, remediate, and investigate information security incidents to maintain and assist in improving the College’s approach to information security risk.
- Develop an informed information security approach, for all areas of the College including learning & teaching, support staff and students.
- Ensure the College is compliant with its information security obligations – especially those related to the hosting, curation, or processing of 3rd party data.
- Provide assurance to other parties that the College has a robust control environment in place to protect information assets through an effective information security management system.

3 Policy Framework

3.1 The College’s information security is managed through this policy and associated policy documents. This provides a flexible and effective platform upon which the College’s information security objectives are met.

3.2 Adherence to this Policy can be met by adopting and complying with the other policies within the College. However, all the policies are designed to be flexible and allow a range of options to meet ongoing requirements. Regardless of the approach, all within scope of the Policy are required to meet the requirements of this Policy.

3.3 It is important to note that all policies are to be considered the minimum requirements for information security (or the ‘baseline’). Where additional information security controls are required for research, legal, regulatory or governance purposes, the controls must be enhanced accordingly.

4 Policy Statement

4.1 The College manages and produces information that may be private, confidential or sensitive in nature, together with information that is regarded as being readily available for general sharing. It should be noted that it is imperative that all information is protected from compromise of confidentiality, integrity, and availability. All within the scope of the Policy must therefore ensure:

i Information assets are identified, classified, and protected in accordance with the policies relating to information and security and data protection. Any security controls which are implemented must be proportionate to the defined classification.

ii All processes, technology, services, and facilities are protected through information security controls as outlined in relevant policies.

iii Information security incidents are identified, contained, remediated, investigated, and reported in accordance with the relevant data protection policy.

iv Where a third-party provider is utilised for any services which involves contact with College information, an information security risk assessment is carried out.

v Where appropriate, a risk assessment is carried out on all processes, technology, services, and facilities in accordance with the associated Standard to manage risk within appetite.

vi Back-up and disaster recovery plans, processes, and technology, are in place in accordance with the Business Continuity Standard to mitigate risk of loss or destruction of information and/or services and to ensure that processes are in place to maintain availability of data and services.

vii Where off-site working takes place, appropriate security controls are implemented in accordance with the associated Standards.

In addition, all individuals within scope of the Policy must:

viii Complete Information Security Awareness Training.

Ix Ensure that reasonable effort is made to protect the College's information and technology from accidental or unauthorised disclosure, modification, or destruction.

5 Compliance/review

5.1 This Policy and associated policies are reviewed on a periodic basis by the Business& Resources Manager to ensure they remain accurate, relevant, and fit for purpose.

5.2 The Data protection Officer may carry out periodic compliance and assurance activities (eg assessment of security controls) to ensure control outcomes are aligned with the Policy Framework.

5.3 Failure to meet requirements detailed within this and associated policies may result in the user being subject to formal disciplinary action that will be dealt with under the appropriate disciplinary code or procedures. Additionally, where it is suspected that an offence has occurred under UK or Scots law, it may also be reported to the police or other appropriate authority.

6 Responsibilities

6.1 The Principal is accountable for ensuring adequate and effective information security controls are in place within the College. They are also accountable for compliance in any subsidiary unit, for example, associated Institutes, research groups or multi-disciplinary organisations within their management. In addition, the following have information security responsibilities:

6.2 The Senior Management Team and any associated Governance committees have executive responsibility for information security within the College. They must actively support the adoption and implementation of the information security requirements as well as ensuring compliance within their areas of responsibility.

6.3 Users are responsible for protecting the College's information and technology systems and for complying with the College Computing Regulations, this Policy and any other associated policies. If a user suspects or discovers any material breach of the requirements detailed within this Policy, they must report this immediately to the Business & Resources Manager. Where an individual user suspects personal data may have been compromised, they must notify the Business & Resources Manager and Data Protection Officer (DPO) through the method detailed in the Data Breach Policy.

6.4 Students must accept that they carry responsibility when utilising the College's facilities, technologies or services and will take all reasonable steps to protect the Colleges' information and technology systems. Students will comply with the College Computing Regulations, this Policy and associated policies, where required.

Newbattle Abbey College	**Policy/Procedure**
Title: Information Security Policy	Policies & Procedures - Organisational
Prepared by: Data Protection Officer/Business & Resources Manager	No of Pages - 4
Approved by: Planning & Resources Committee	April 2021
Date approved:	Revision date: April 2023