Newbattle Abbey College
Colaiste Abaid a'Bhatail Nuaidh

NEWBATTLE ABBEY COLLEGE
INFORMATION SECURITY POLICY

1. Purpose and Scope

The Information Security Policy (the "Policy") sets out the 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.

1.1 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.

1.2 This policy applies to all information assets, including verbal communications, hardcopy documents, data, software, storage media, web-based and remotely hosted services, hardware and communications networks and the buildings within which such assets exist.

1.3 This Policy is managed and developed by the Director of Operations on behalf of the College.

1.4 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 and students. 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.
- Third-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, third-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 Colleges approach to information security risk.
- Develop an informed information security approach, for all areas of the College, including 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 third-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 (see Appendix II). 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 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 those 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 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 Breach of Data 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 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 Director of Operations to ensure they remain accurate, relevant, and fit for purpose.

5.2**.** The Data Protection Officer may carry out periodic compliance and assurance activities (e.g. 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 Audit and Risk Committee of the Board of Directors provides advice and sources of assurance to the Board of Directors on the adequacy and effectiveness of the College Risk Management systems. This includes overseeing the policies and systems relating to information security.

6.1. The Principal is accountable for ensuring adequate and effective information security controls are in place within the College.

6.2. The Senior Management Team have executive responsibility for information security within the College.

6.3 College managers must actively support the adoption and implementation of the information security requirements, as well as ensuring compliance within their areas of responsibility.

6.4 All users are responsible for protecting the College's information and technology systems and for complying with 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 Director of Operations or a member of the senior management team. Where an individual user suspects personal data may have been compromised, they must notify the Director of Operations and Data Protection Officer (DPO) through the method detailed in the Data Protection Policy.

6.5 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 this Policy and associated policies, where required.

Appendix I

Policies and procedures relevant to information security:

- Data protection policy
- Breach of Data Policy
- Policy on the secure handling, use, storage, retention and destruction of disclosure information
- Data Retention Policy
- Computer users agreement
- Email Policy
- Disaster recovery and business continuity policy and procedure
- CCTV Policy

Newbattle Abbey College	**POLICY/PROCEDURE**
Title: Information Security Policy	File ref: Organisational
Lead officer: Data Protection Officer	No of pages: 9
Approved by: Audit & Risk Committee	Date last reviewed: n/a
Date first approved: May 2024	Next Revision date: May 2027

Single Equality Scheme Impact Assessment Initial Screening

<table>
<tr><td colspan="2"><b>1. Title of Proposal/Policy/Procedure: Information security policy</b></td></tr>
<tr><td><b>Is this:</b>
A revised Proposal/Policy/Procedure □
A new Proposal/Policy/Procedure x</td><td><b>Lead Officer: Mike O’Donnell, DPO / Roddy Henry, Principal</b>
(Name and job title)</td></tr>
<tr><td><b>Description:</b>
(Briefly, but clearly, describe the purpose of the proposal/policy/procedure including its aims, objectives and intended outcomes)</td><td>The Information Security Policy sets out the College’s 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.</td></tr>
<tr><td colspan="2"><b>2. Relevance to the Equality Act 2010: Yes □ No x</b></td></tr>
<tr><td colspan="2"><b>Does the Proposal/Policy/Procedure have any relevance under the Equality Act 2010?</b>
<i>(If yes – indicate ‘Yes’ (above) and fully complete the remainder of Section 2. If the Proposal/Policy/Procedure has no relevance under the Act, please select “No” and go to Section 3.)</i></td></tr>
</table>

<table>
<tr><td colspan="5"><b>Which groups of people do you think will be or potentially could be, impacted by the implementation of this proposal/policy/ procedure? (You should consider employees, clients, students, and any other relevant groups)</b></td></tr>
<tr><td colspan="5">Please tick below as appropriate (against each of the nine equality groups) to indicate any impact, and provide a brief explanation.</td></tr>
<tr><td rowspan="2"></td><td colspan="3"><b>Impact</b></td><td rowspan="2"><b>Please explain the potential impacts and how you know this</b></td></tr>
<tr><td><b>None</b></td><td><b>Positive</b></td><td><b>Negative</b></td></tr>
<tr><td><b>Age:</b> A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).</td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>Disability:</b> A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.</td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>Gender Reassignment Trans/Transgender Identity:</b> The process of transitioning from one gender to another.</td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>Marriage or Civil Partnership:</b> Marriage is a union between a man and a woman or between a same-sex couple.
Same-sex couples can also have their relationships legally recognised as 'civil partnerships'. Civil partners must not be treated less favourably than married couples (except where permitted by the Equality Act).</td><td></td><td></td><td></td><td></td></tr>
</table>

Pregnancy and Maternity: Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.				
Race: Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.				
Religion or Belief: Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.				
Sex: A man or a woman.				
Sexual Orientation: Whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes.				

3. Full Equality Impact Assessment

Full Equality Impact Assessment Required? (Select No if you have answered 'No' or "None" to all of Section 2)	**Yes ☐ No x**
If a full Equality Impact Assessment is <u>not</u> required, please provide a brief explanation below.	
The policy has no impact in terms of equalities.	

Signed by (Lead Officer):	**Roddy Henry**
Designation:	**Principal**
Date:	**December 2024**
Counter Signature: (Incl. designation)	
Date:	