Newbattle Abbey College
Colaiste Abaid a'Bhatail Nuaidh

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) ACCEPTABLE USE POLICY

1. Purpose and Scope

This policy establishes acceptable use standards for all Information and Communication Technology (ICT) resources and services provided by Newbattle Abbey College. It applies to all staff, students, contractors, visitors, and any other users of College ICT systems and equipment.

ICT resources include but are not limited to: computers, laptops, tablets, mobile devices, network infrastructure, cloud services (including Microsoft 365), internet access, software applications, data storage systems, and any other technology provided or managed by the College.

2. General Principles

College ICT resources are provided primarily to support educational, administrative, and research activities. Users must:

- Use ICT resources responsibly, ethically, and in compliance with all applicable laws and College policies
- Respect the rights and privacy of others
- Maintain the security and integrity of College systems and data
- Use resources efficiently and avoid wasteful practices
- Report security incidents or policy violations promptly to ICT Services

3. User Responsibilities

3.1 Account Security

Users are responsible for maintaining the security of their accounts and must:

- Keep passwords confidential and never share them with others
- Use strong passwords (minimum 12 characters with uppercase, lowercase, numbers, and symbols)
- Enable Multi-Factor Authentication (MFA) when available
- Change passwords immediately if compromise is suspected
- Lock workstations when leaving them unattended (Windows Key + L)
- Log off completely when finishing a session, especially on shared computers
- Report lost or stolen devices immediately to ICT Services

3.2 Data Protection and Privacy

Users must comply with the college Data Protection Policy

3.3 Software and System Integrity

- Only use licensed software authorised by the College
- Never install unauthorised software or applications on College devices

- Not attempt to bypass, disable, or circumvent security controls or monitoring systems
- Not modify system configurations without authorisation from ICT Services
- Maintain up-to-date anti-virus protection (managed by ICT Services)
- Apply security updates and patches as prompted

4. Acceptable Use

ICT resources are provided primarily for educational, training, administrative, and research purposes. Limited personal use is permitted provided it:

- Does not interfere with work or study responsibilities
- Does not compromise system security or performance
- Does not consume excessive resources (bandwidth, storage, processing)
- Complies with all other provisions of this policy
- Does not bring the College into disrepute

5. Prohibited Activities

The following activities are strictly prohibited when using College ICT resources:

5.1 Illegal or Harmful Content

- Accessing, creating, storing, distributing, or transmitting illegal content
- Accessing, storing, or distributing offensive, obscene, indecent, or discriminatory material
- Viewing, downloading, or distributing content depicting child abuse or exploitation
- Content that promotes violence, terrorism, or extremism
- Content that harasses, bullies, or intimidates others (including cyberbullying)

5.2 Unauthorised Access and Malicious Activity

- Attempting to gain unauthorised access to College systems or other users' accounts
- Deliberately introducing malware, viruses, or other malicious code
- Conducting network attacks, port scanning, or penetration testing without authorisation
- Intercepting or monitoring network traffic without authorisation
- Using College resources for cryptocurrency mining
- Attempting to circumvent network security or content filtering

5.3 Misuse of Resources

- Using College resources for commercial gain or private business activities
- Online gambling or accessing gambling websites
- Excessive streaming of non-educational media content

- Downloading or distributing pirated software, media, or copyrighted material
- Sending spam, chain emails, or participating in pyramid schemes
- Using College systems to impersonate others or forge communications

6. Internet and Web Use

Internet access is provided to support College activities. Users should be aware that:

- Web filtering is in place to block inappropriate content and comply with legal obligations
- Internet usage may be monitored and logged for security and compliance purposes
- Users must respect copyright and intellectual property rights when downloading or sharing content
- Social media use should follow any college policies relating to social media or digital communications

7. Social Media and Online Conduct

When using social media (including platforms such as Facebook, X, Instagram, LinkedIn, TikTok, YouTube, etc.) on College systems or in a way that may be associated with the College, users must:

- Be respectful and professional in all online interactions
- Clearly indicate when expressing personal opinions that do not represent the College
- Not share confidential College information, student data, or unpublished research
- Not post content that could damage the College's reputation
- Respect copyright and intellectual property when sharing content
- Follow any college policies relating to social media or digital communications
- Report cyberbullying, harassment, or inappropriate content to appropriate staff

8. Mobile Devices and Remote Access

- College-owned mobile devices must be secured with passwords/biometric authentication
- Personal devices accessing College data must comply with security requirements (see Section 11)
- Lost or stolen devices must be reported immediately
- Remote access to College systems must only use approved methods (VPN, RDP, etc.)
- Personal devices should not be used for College business unless enrolled in an approved Bring Your Own Device (BYOD) programme (see Section 11)
- Mobile devices must not be used while driving

9. Cloud Services and External Storage

- Use College-approved cloud services (primarily Microsoft 365/OneDrive/SharePoint)
- Do not store College data on unauthorised cloud services or personal accounts
- Ensure sensitive data is encrypted when stored on portable media
- Back up important files to OneDrive for Business or SharePoint
- Understand that personal cloud storage services may not meet data protection requirements

10. Monitoring and Privacy

The College reserves the right to monitor ICT resources for security, performance, and compliance purposes. Monitoring may include:

- Network traffic analysis and logging
- Email and communications monitoring (in accordance with legal requirements)
- Internet usage tracking and web filtering logs
- System access logs and user activity
- Security scanning and threat detection

The Organisation's IT systems, including email accounts and stored files, are provided for business purposes and remain the property of the Organisation at all times. Users should not consider any communications or data held on these systems to be private. Personal communications will be respected where possible, but the College may need to access accounts for legitimate business reasons, security investigations, or legal requirements. Any such access will be proportionate, legitimate and will be conducted in compliance with data protection legislation and relevant regulations. Only the Principal or his/her designated Depute may authorise such access.

11. Bring Your Own Device (BYOD)

Personal devices may be used to access College resources only if they meet the following requirements:

- Devices must be protected with passwords or biometric authentication
- Devices must have current operating systems and security updates
- Anti-virus/anti-malware software should be installed and current
- The College is not responsible for damage, loss, or theft of personal devices
- The College may require personal devices to be wiped if they pose a security risk
- Users must comply with all other provisions of this policy when using personal devices

12. Legal Compliance

Users must comply with all applicable laws and regulations, including but not limited to:

- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Communications Act 2003
- Equality Act 2010
- Protection from Harassment Act 1997
- Investigatory Powers Act 2016
- Online Safety Act 2023
- JANET Acceptable Use Policy (for further education network access)

13. Incident Reporting

Users must report the following to ICT Services immediately:

- Suspected security breaches or unauthorised access
- Lost or stolen devices containing College data
- Suspected malware infections or unusual system behavior
- Phishing attempts or suspicious emails
- Data breaches or accidental disclosure of sensitive information
- Observed violations of this policy
- Technical issues affecting security or availability

Contact ICT Services at: [ICT Email Address] or [IT Support System]

14. Consequences of Policy Violations

Violations of this policy may result in disciplinary action under relevant college policies

15. Policy Arrangements

Please refer to the College 'Policies and Procedures Lists and Status' for review timetable.

This Plan 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:	Information and Communication Technology (ICT) Acceptable Use Policy
Lead Officer:	Depute Principal
Date last reviewed	October 2026
Next Review date:	October 2029
Approved By:	Board
Date first approved:	October 2026