Acceptable Use Policy

New College Durham is committed to safeguarding & promoting the welfare of children and young people, as well as vulnerable adults, and expects all staff and volunteers to share this commitment.

Policy Title	**Acceptable Use Policy**
Document Owners	**Executive Director of ICT and Corporate Services / Head of ICT**

Directorates and Departments affected by this Procedure	**All Staff, Students and Third Parties using the College IT facilities.**
Procedure Effective From	**July 2026**
Next Review Date	**July 2031**

Contents

We will consider any request for this procedure to be made available in an alternative format.

We review our policies and procedures regularly to update them and to ensure that they are accessible and fair to all. All policies and procedures are subject to equality and accessibility impact assessments.

We are always keen to hear from anyone who wants to contribute to these impact assessments, and we welcome suggestions for improving the accessibility or fairness of the policy.

Equality Impact Assessed: July 2026

Accessibility Checked: July 2026

1. Introduction

This Acceptable Use Policy (AUP) outlines the rules and guidelines for the appropriate use of information technology (IT) facilities provided by New College Durham. It is essential that all users understand and adhere to these guidelines to ensure a secure and productive computing environment.

2. Scope and Purpose

This policy applies to all staff, students, contractors, consultants, external agency staff and guests who have access to New College Durham IT facilities, including computers, networks, and associated resources. A registered user may use the College network and computer equipment for any legal activity that is in furtherance of the aims and policies of the College. In registering, a user accepts the terms of the College's Cyber Security Policy, Web and Intranet Management Policy, Management and Monitoring of Electronic Communications, Internet and Telephones Policy Information Security Policy and the Data Protection Policy and undertakes to comply with the statements within this policy. This policy should also be read alongside the College's Safeguarding Children and Adults at Risk Policy and Procedure, which sets out the College's approach to online safety, filtering and monitoring, and the reporting of safeguarding concerns.

3. Users

a. Staff

College staff are responsible for familiarising themselves with this Policy. Staff are responsible for ensuring IT resources allocated to them or used by staff and students in the classroom, are stored securely and kept in a good state of repair. Staff should ensure equipment is adequately charged and securely locked away when not in use. Damaged/ faulty equipment must be reported to the Information and Communication Technology (ICT) Department immediately including any incidents of equipment being deliberately damaged or defaced.

b. Students

A student confirms acceptance of this AUP by enrolling with the College. Once a student enrolment is confirmed, user privileges are conferred and compliance with this AUP will be in place for as long as user privileges are extended. Students are informed of their obligations when they are supplied with their network account.

c. Third Parties

Third parties are provided with access privileges when engaged via the College procurement process, the College Health and Safety process and/or the HR process for the engagement of external staff. Third party users accept the terms of the policy when accessing College systems. They must not access or copy personal or confidential data without explicit authorisation. If access to such data is required, a data sharing agreement must be completed.

d. System Support Accounts

Access to individual College application systems is given to the supplier of an IT system for the purposes of maintenance, upgrade, and fault rectification. The terms of this AUP are agreed by the consultant when accessing the College network. The supplier may only use their network credentials for the purpose of maintaining, upgrading, and supporting the system. The College purchasing Terms & Conditions defines suppliers as 'Processors' with respect to the College personal data. Service account credentials will be disabled when not in active use.

All users share responsibility for maintaining a safe online environment. Any concerns relating to online safety, inappropriate online content, cyberbullying, suspected grooming, extremist material or any safeguarding concern encountered whilst using College ICT systems must be reported immediately in accordance with the College Safeguarding Children and Adults at Risk Policy and Procedure.

4. Responsibilities

All users have a responsibility to abide by this Policy and if they are uncertain about any of the obligations detailed, they must seek clarity from the Executive Director of ICT and Corporate Services or the Head of ICT.

All users must ensure they are aware of their obligations under this policy and that any concerns are directed to the Executive Director of ICT and Corporate Services.

5. User Login and Password

All users who require access to the College Network are required to have a legitimate user login and password. Users must adhere to the following:

- Do not attempt to gain unauthorised access to College IT systems.
- Passwords must never be written down or disclosed to another individual or organisation.
- Do not use passwords which are easily guessed e,g, Password 123
- Passwords must be strong including upper- and lower-case letters, numbers, symbols.

6. Network Security

Users must not attempt to compromise the security of the college network or any connected systems. Unauthorised scanning, probing, or monitoring of network traffic is strictly prohibited.

7. Respect for Privacy

Users are expected to respect the privacy of others and not attempt to access or disclose personal or confidential information without proper authorisation. Use of IT facilities for harassment, bullying, or any form of malicious intent towards others is strictly prohibited.

All users are required to comply with relevant Data Protection Principles as described in the College Data Protection Policy.

Users must not share any confidential information belonging to the College.

8. Copyright and Intellectual Property

Users must respect copyright laws and intellectual property rights. Unauthorised distribution or sharing of copyrighted materials is not allowed. Software installation and use must comply with license agreements.

9. Communication Tools

Communication tools such as Teams, Outlook email and telephone should be used for college-related communication. Users should not engage in spamming or any form of email or online abuse. Users must only use College network accounts for legitimate College business and authorised College activities. College network accounts must not be used to undertake official business on behalf of another organisation unless this has been formally approved by the College and any necessary information governance arrangements are in place. Permission from another organisation does not constitute authorisation to use College ICT systems.

Users must communicate respectfully and professionally when using College ICT systems. The use of electronic communications, collaboration platforms, social media or AI-generated content to harass, bully, intimidate, discriminate against or otherwise cause harm to another individual is prohibited.

Users must not use mobile devices or College ICT systems to photograph, video record or audio record learners, colleagues or visitors unless there is a legitimate College business purpose and appropriate authorisation.

10. Prevent

Under the College Prevent Duty, users utilise our systems on the clear understanding that they will do nothing that will be contrary to the prevailing legislation notably The Terrorism Act (2006) outlaws web posting of material that encourages or endorses terrorist acts, even terrorist acts carried out in the past. Indeed, sections of the Terrorism Act also create a risk of prosecution for those who transmit material of this nature, including transmitting this material electronically. Visits to any websites related to terrorism and/or downloading of material issued by such groups (even from open access sites) is subject to monitoring by the College and will be reported to the appropriate authority.

11. Unauthorised Use

Use of IT resources for illegal activities, including but not limited to hacking, unauthorised access, or distribution of malicious software, is strictly prohibited.

Examples of the more common activities that users must not carry out are: (N.B this is not an exhaustive list):

- deliberately attempt to gain access to restricted areas within the College or other locations.
- visit, view, transmit or download any internet material which is counter either to legislation, College policies (eg equal opportunities, bullying and harassment) or to commonly accepted standards, or is likely to be offensive or indecent to reasonable people. This includes inappropriate websites including those promoting extreme Islamic or right-wing ideologies as well as material concerning the purchase of firearms. Members of staff may access this kind of material only with prior permission when for bona fide academic purposes.
- the creation or transmission of material which is designed or likely to cause annoyance, inconvenience, or needless anxiety.
- the download, copying or transmission to third parties the works of others without their permission. Written material, images and software are protected by the laws on copyright.
- When using communication tools such as email, Teams etc, user should not engage in spamming or any form of email or online abuse.
- Users must not use college network accounts for personal commercial activities or any other non-educational purposes.
- the transmission of unsolicited commercial material.
- corrupting or destroying other users' data.
- violating the privacy or disrupting the work of others.
- using the network in a way that denies service to other users, for example, deliberate or reckless overloading of the network or computers.
- deliberately introducing viruses onto the College network.
- place on the Internet any material, which incites, encourages, or enables others to gain unauthorised access to the College's computer system.
- introduce data-interception, password-detecting or similar software or devices to the network.
- use the College data or systems to defraud, blackmail or otherwise carry out unlawful acts.
- access or copy personal or confidential data without the explicit authorisation of the College.
- process personal data on behalf of another organisation using College ICT systems unless the College has formally approved this.
- forward College emails or attachments containing personal data, confidential information or commercially sensitive information to personal email accounts or personal cloud storage services unless there is an approved business requirement and appropriate authorisation.
- use College ICT systems to store or process information belonging to another organisation where appropriate contractual or data sharing arrangements have not been established.

- use College ICT facilities in a manner that could result in the College processing personal data without an appropriate lawful basis.
- install hardware on an individual PC.
- attach devices to an individual PC or VDI.
- subscribe to internet services via the College network.
- load, install or modify software.
- encrypt data (the College will remove any encrypted data from the systems).
- remove equipment from its location without authorisation.
- damage or deface equipment.
- Export data to systems external to the college excluding authorised partners.
- Breach Data protection obligations.
- Create, use, possess or distribute artificial intelligence (AI) generated, manipulated or synthetic images, audio, video or text (including deepfakes) where the purpose or effect is to harass, bully, intimidate, impersonate, deceive, exploit or otherwise cause harm to another individual.
- create, request, possess, transmit or share AI-generated, digitally manipulated or synthetic nude or semi-nude images of any person without their explicit consent, or where doing so would be unlawful, abusive or constitute a safeguarding concern.
- use AI or other digital technologies to impersonate another individual, misrepresent their identity or create false or misleading content intended to deceive others or damage the reputation of an individual or the College.
- use College ICT systems or networks to generate, access, store or distribute content that promotes or facilitates abuse, online harassment, hate, discrimination, extremism, violence, sexual exploitation or other harmful behaviour.
- upload confidential, personal or commercially sensitive College information into publicly available AI services or other external digital platforms without explicit College authorisation.
- use AI technologies in any manner that breaches College policies relating to safeguarding, equality, dignity and respect, academic integrity, information security or data protection.

The College regards the misuse of artificial intelligence, including the creation or sharing of AI-generated or manipulated content that causes harm to others, as a serious safeguarding matter. Such misuse may constitute child-on-child abuse, online harassment, sexual harassment, bullying, discrimination, or criminal behaviour and will be investigated under the College's disciplinary procedures. Where appropriate, matters may be referred to the Designated Safeguarding Lead, the Police, or other external agencies.

12. Monitoring

The College reserves the right, without notice, to access, listen to or read any communication you make or receive using College facilities. The College operates filtering and monitoring technologies to help safeguard learners, staff and College systems from inappropriate, harmful or illegal online content and activity. Users should have no

expectation of privacy when using College ICT systems beyond that provided by law and College policies. It will only do this for the following purposes:

- to establish the existence of facts
- to ascertain compliance with regulatory or self-regulatory practices and procedures
- to investigate or detect unauthorised use of systems.
- to prevent or detect crime.
- to provide practical help to prevent people from being drawn into terrorism and violent extremism.
- to intercept for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding e mails to correct destinations.
- to check electronic communications systems when you are on holiday or on sick leave.

Monitoring will only be undertaken by authorised personnel who understand the College's obligations under prevailing Data Protection Regulations.

13. Artificial Intelligence (AI)

Artificial Intelligence (AI) encompasses technologies and techniques that enable computers to perform tasks that typically require human intelligence. These tasks include problem-solving, understanding natural language, recognising patterns, learning from experience, and adapting to changing circumstances.

When using AI tools, the user must ensure they maintain ethical research and development, privacy, security, and lawful responsibilities.

The following activities involving AI systems are strictly prohibited:

- Engaging in activities that compromise the security or integrity of AI systems.
- Using AI to perpetrate fraud, deception, or other forms of malicious behaviour.
- Discriminatory or biased use of AI that may harm individuals or communities.
- Creating or disseminating harmful content generated by AI, including deepfakes or misinformation.
- upload College personal data, confidential information or commercially sensitive information into publicly available AI services unless this has been approved by the College.

The College may monitor the use of AI services on its ICT systems to ensure compliance with this policy and to protect College information, learners and staff. Users remain responsible for verifying the accuracy and appropriateness of AI-generated content before relying upon or sharing it. AI must not be used in a way that places learners at risk or creates, distributes or promotes harmful, misleading or inappropriate content.

14. Policy Compliance

Any misuse of IT facilities or breaches of this policy will be reported to the appropriate Senior Leader. Failure to adhere to this policy may result in formal action under the college's prevailing procedures, including access restrictions, and could lead to further legal consequences if security breaches occur due to non-compliance. If the misuse breaches current law or is reportable under relevant legislation the College reserves the right to inform the police or relevant authority.

15. Evaluation and Review

The effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.