



IT Acceptable Use Policy (Students)

September 26

Content

1) Introduction and Scope	3
2) General Rules for IT Use	3
2.1 Acceptable Use	3
2.2 Prohibited Activities:	3
3) Online Conduct and Communication	3
3.1 Responsible Communication:	3
4) Safety and Privacy:	3
4.1 To protect yourself and others:	3
4.2 Account and Device Security	4
5) Software, AI, and Copyright	4
5.1 Software Use:	4
5.2 Artificial Intelligence (AI):	4
6) Monitoring and Consequences	4
6.1 Monitoring:	4
6.2 Breaches of Policy:	4
7) Document Change Control:	6
8) Document Control Information:	6
9) Related Policies	6

1) Introduction and Scope

The purpose of this policy is to ensure all college IT facilities are used safely, lawfully, and fairly to support effective learning, teaching, and business functions. By using any college IT facilities—including computers, software, cloud services and networks on any device (college-owned or personal)—you agree to be bound by these rules. This policy applies to all students and should be read alongside the Nescot Code of Conduct and Behaviour Policy, the Sexual Harassment Policy, and the College Code of Conduct for Protecting Free Speech.

2) General Rules for IT Use

2.1 Acceptable Use

The IT network is for college-related work, educational activities, and responsible communication with students, staff, and external organisations related to your course.

2.2 Prohibited Activities:

You are strictly forbidden from:

- Disrupting the system or others' work by introducing viruses, hacking, or trying to bypass security protocols.
- Damaging or disabling IT equipment.
- Using the network for commercial purposes, like selling things, or for non-college activities that strain the network, such as playing games or bitcoin mining.
- Loading your own software without written permission.
- Eating or drinking near IT equipment.
- Connecting personal devices to any network other than Eduroam.

3) Online Conduct and Communication

3.1 Responsible Communication:

You must not use threatening, abusive, obscene, racist, or degrading language in any communication, including on social media. While Nescot upholds freedom of speech, expression that constitutes unlawful harassment, hate speech, defamation, or incitement to violence is strictly prohibited.

3.2 Cyberbullying:

Cyberbullying, harassment, online stalking, and sending unwelcome sexual advances are serious offences. Any student found responsible for cyberbullying will be subject to the college's disciplinary procedures.

4) Safety and Privacy:

4.1 To protect yourself and others:

- Do not share personal information like your address or phone number.

- Do not become online "friends" with or arrange to meet people you don't know in real life.
- Report any accidental access to inappropriate material to IT Services.
- Do not create or share propaganda for extremist causes or material intended to radicalise others, in line with the Prevent Duty.

5.1 Account and Device Security

User Accounts:

- Your unique user account is your responsibility. You must never share your account details or allow anyone else to use your account. IT Services will never ask for your password.

Password Security:

- Create a strong, unique password (at least 12 characters with a mix of uppercase, lowercase, numbers, and symbols). Do not write it down or use the same password for other services. Using a passphrase or a password manager is recommended.

Remote Access:

- When accessing college services like Microsoft 365 from personal devices, you must ensure your device is secure, updated, and running malware protection. Avoid using unsecured public Wi-Fi and do not save sensitive college data on personal devices. By connecting your personal device you agree to submitting it for random audits when required.

5) Software, AI, and Copyright

6.1 Software Use:

College software must not be used for commercial or personal purposes. You must adhere to all copyright and licensing agreements, which prohibit unauthorised copying, sharing, or reverse engineering of software.

5.2 Artificial Intelligence (AI):

- AI tools may be used to support learning but must not be used for academic misconduct, such as plagiarism. Do not input personal or sensitive information into AI tools. All use must comply with the Students' Guidelines for AI and the Academic Integrity Policy.

6) Monitoring and Consequences

7.1 Monitoring:

Be aware that all internet and cloud service usage on owned and maintained by the college is logged and may be monitored by system administrators without your knowledge. All data, files, and emails on the system are considered college property.

8.1 Breaches of Policy:

Any violation of this policy is taken very seriously and may result in disciplinary action, including warnings, suspension, or permanent exclusion. Serious breaches include accessing obscene content, cyberbullying, hacking, or creating material intended to radicalise. You must also comply with relevant laws like the Data Protection Act and the JANET Acceptable Use Policy, which can be found on the Jisc website.

7) Document Change Control:

Author	Version	Date Issued	Change
Director of IT and Data Service	0.1	01/11/2024	First Draft
Director of IT and Transformation	0.2	17/07/2025	Second Draft
Assistant Principal, Head of Governance, Head of Quality Improvement and Innovation	0.3	22/09/2025	Third Draft
Head of IT	0.4	22/06/2026	2026 updates

8) Document Control Information:

Version	v.2
Policy Originator	Director of IT and Transformation
Approved by	CLT
Review Interval	1 Year
Last Review Date	22/07/2026
Next Review Date	20/07/2027
Audience	Public
Entered on SharePoint	Autumn 2026
Entered on Website	Autumn 2026

9) Related Policies

- Nescot Code of Conduct and Behaviour Policy
- Nescot Sexual Harassment Policy
- Nescot Code of Conduct for Protecting Free Speech
- Nescot Equality, Diversity and Inclusion Policy
- AI and the Academic Integrity Policy

Online safety and safeguarding

Use of College systems must support a safe learning environment.

- Users must not create, access, store or share material connected with child sexual abuse, grooming, criminal exploitation, extremist radicalisation, hate crime or other unlawful harm. Accidental exposure must be reported immediately to IT Services or the Safeguarding and Wellbeing Team.
- Concerns about online grooming, exploitation, coercion, threats, harmful content or the safety of any student must be reported under the Safeguarding Policy. The College may preserve and share relevant records where required for safeguarding, legal or regulatory purposes.

Generative artificial intelligence

AI may support learning only where its use is permitted by the relevant teacher, assessment rules and College guidance.

- Students remain responsible for the accuracy, quality, lawfulness and originality of submitted work, including checking for bias, fabricated information and incorrect references.
- AI-generated material must be acknowledged where required. Using AI to misrepresent authorship, evade assessment rules or gain an unfair advantage may constitute academic misconduct.
- Personal, confidential, commercially sensitive, safeguarding or special category data must not be entered into public AI services unless the College has expressly approved the service and use.

Monitoring, privacy and proportionality

The College monitors and logs use of its networks, devices and cloud services for cyber security, safeguarding, service management, legal compliance and investigation of suspected misuse. Monitoring will be authorised, necessary and proportionate, and personal data will be handled under the College Privacy Notice, UK GDPR and the Data Protection Act 2018.

- College systems should not be treated as private. Monitoring does not remove the College duty to handle personal data fairly and securely.
- A student who believes monitoring or a sanction has been applied unfairly may use the College Feedback, Compliments and Complaints Policy. Disciplinary appeals remain governed by the applicable student disciplinary procedure.

Legal and policy framework

This policy should be read with the College Safeguarding Policy, Privacy Notice, Academic Integrity Policy, Student Behaviour Policy and complaints procedure.

- Computer Misuse Act 1990; Data Protection Act 2018 and UK GDPR; Copyright, Designs and Patents Act 1988;

Counter-Terrorism and Security Act 2015; Equality Act 2010; and the current Keeping Children Safe in Education guidance.