



Nenagh College



Internet Acceptable Use Policy

Date of Commencement: 1st January 2026

Policy Area	Schools
Document Reference number	NEN/ICT/023/1
Version	1
Document Drafted by	Nenagh College
Date previous version Adopted by BOM Noted by TETB	3 December 2024 20 May 2025
Date Reviewed/Amended by School	December 2025
Date Reviewed/Ratified by BOM	11 December 2025
Date Noted/to be Noted by TETB	27 January 2026
Policy Review Date	Every Two Years
Date of Withdrawal of Obsolete Document	01.01.2026 Document Ref. No. NEN/ICT/023/0 Version No. 1

CONTENTS

Preamble	4
Content Filtering	5
Internet Use	5
Email and Messaging	6
Social media and messaging services	7
Data Protection and Security	8
Session Management.....	9
Prearranged Live 1:1 Sessions.....	9
Behaviour Expectations	10
Policy Breaches and Reporting Concerns	10
Artificial Intelligence (AI) Use in School.....	11
Personal Devices	12
Digital Learning Platforms (including video conferencing).....	12
Images and Video.....	12
Inappropriate Activities	13
School Websites.....	14
Cyberbullying	14
Legislation	15
Support Structures.....	15
Sanctions	16
APPENDIX 1.....	17

Preamble

The aim of this Acceptable Use Policy is to ensure that students will benefit from learning opportunities offered by the school's digital resources in a safe and effective manner. The responsible use of internet and digital technologies, both online and offline and access, is considered an integral part of teaching and learning. Therefore, if the school AUP is not agreed, sanctions will be imposed.

It is envisaged that school and parent representatives will revise the AUP at least annually. Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

When using the internet students, parents and staff are expected:

- To always treat others with respect.
- Not undertake any actions that may bring the school into disrepute.
- Respect the right to privacy of all other members of the school community.
- Respect copyright and acknowledge creators when using online content and resources.

The school employs several strategies to maximize learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

Filtering software and/or equivalent systems will be used to minimize the risk of exposure to inappropriate material.

- Uploading and downloading of non-approved software will not be permitted.
- The use of personal external digital storage media in school requires school permission.
- Virus protection software will be used and updated on a regular basis.

This Acceptable Use Policy applies to students who have access to and are users of the internet in Nenagh College.

This policy also applies to members of staff, volunteers, parents, carers and others who access the internet in Nenagh College.

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

Nenagh College implements the following strategies on promoting safer use of the internet:

- Pupils will be provided with education in internet safety as part of our implementation of the SPHE and other curriculum areas.

- Internet safety advice and support opportunities are provided to pupils in Nenagh College through our Induction, Pastoral Care, Coding and Digital Media Literacy programmes.

This policy and its implementation will be reviewed by the following stakeholders:

- Board of Management
- parents
- teaching staff and
- pupils.

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (including sites visited).
- Surveys and/or questionnaires of pupils, parents, and teaching staff.

Should serious online safety incidents take place, the Principal, Deputy Principal and Digital Coordinator should be informed.

The implementation of this Internet Acceptable Use policy will be monitored by the Deputy Principal and Digital Coordinator.

Content Filtering

Nenagh College has chosen to implement the following level on content filtering on the Schools Broadband Network:

Level 4 This level allows access to millions of websites including games and YouTube but blocks access to websites belonging to the personal websites category and websites such as Facebook belonging to the Social Networking category.

Students taking steps to bypass the content filter by using proxy sites or other means may be subject to disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion.

Internet Use

Students will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.

Students will be encouraged to report accessing inappropriate materials accidentally in accordance with school procedures.

Students will report accidental access of inappropriate materials in school but outside the classroom to the Digital Coordinator or Deputy Principal.

Students will not copy information into assignments and fail to acknowledge the source including generative AI (plagiarism and copyright infringement).

Students and staff will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Students will use the Internet for educational purposes only.

Students will not engage in online activities such as uploading or downloading large files that result in heavy network traffic which impairs the service for other internet users.

Students will not download or view any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

Students downloading materials or images not relevant to their studies is in direct breach of the school's acceptable use policy.

Students will never disclose or publicize personal information or passwords.

Students will be aware that any usage of the internet and school's digital platform, including distributing or receiving information, school-related or personal, will be monitored.

Use of file sharing and torrent sites is allowed with staff permission.

Email and Messaging

Students may not download materials or images that are not relevant to their studies.

Students will use approved school email accounts. Students must only use their school email for school related activities and for registering on school-based activities only. The use of personal email addresses is not allowed for school-based work. The use of personal email addresses is only permitted with the permission of school management.

Students should not under any circumstances share their email account login details including passwords with other pupils.

Students should not use school email accounts to register for online services such as social networking services, apps, and games.

Students should be aware that email communications are monitored.

Students will not send any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

Students should immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Students should report any such communications to a teacher.

Students should avoid opening emails that appear suspicious. If in doubt, pupils should ask their teacher before opening emails from unknown senders.

Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.

Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.

Students will note that sending and receiving email attachments is subject to permission from their teacher.

Students will not forward email messages or screenshots of emails or "reply all" without the permission of the originator.

All emails and opinions expressed in email are the responsibility of the author and do not reflect the opinion of the school.

Social media and messaging services

The internet provides a range of social media tools that allow us to interact and keep in touch. While recognizing the benefits of these media for new opportunities for communication, this policy sets out the principles that members of your school community are expected to follow when using social media.

The principles set out in this policy are designed to help ensure that social media is used responsibly so that the confidentiality of pupils and other staff and the reputation of the school is protected.

This policy applies to personal websites such as social networking sites (for example Instagram and TikTok), blogs, microblogs such as X, chatrooms, forums, podcasts, open access online encyclopedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and YouTube. The internet is a fast-moving technology, and it is impossible to cover all circumstances or emerging media.

The following statements apply to the use of messaging, blogging and video streaming services in Nenagh College:

The use of instant messaging services and apps including Snapchat, WhatsApp, Viber, etc. is not allowed for students at Nenagh College.

Use of blogs such as WordPress, Tumblr etc. is allowed in Nenagh College with express permission from teaching staff.

Use of video streaming sites such as YouTube and Vimeo etc. is permitted with express permission from teaching staff.

Members of the school community must not use social media, messaging services and the internet in any way to harass, impersonate, insult, abuse or defame others.

Staff and students must not discuss personal information about pupils, staff and other members of the Nenagh College community on social media.

Staff and students must not use school email addresses for setting up personal social media accounts or to communicate through such media.

Staff and students must not engage in activities involving social media which might bring Nenagh College into disrepute.

Staff and Students must not represent your personal views as those of Nenagh College on any social medium.

Students will be provided with guidance on etiquette regarding social media.

Teachers can read further information about the use of social media and Electronic Communication here:

<https://www.teachingcouncil.ie/en/news-events/latest-news/2021/guidance-for-registered-teachers-about-the-use-of-social-media-and-electronic-communication.html>

Data Protection and Security

Nenagh College will continue to follow the guidance outlined in Tipperary ETB's Data Protection policy.

All participants will be made aware that the Microsoft platform records activity.

Staff or students will not record lessons or meetings using personal equipment unless agreed and risk assessed by the principal.

Only members of the Nenagh College community will be given access to the school's Microsoft platform. If outsiders who need access to enhance the educational experience of students are being given temporary access to the system this will be approved by the principal.

It is expected that all users will use strong passwords and log off or lock devices when not in use.

Session Management

Staff will record the attendance at live sessions using VS ware.

Appropriate privacy and safety settings will be used to manage access and interactions. This includes:

Students will only be permitted to share screens with explicit permission of teachers and teachers will turn off Teams for the classroom when not in use.

Live streaming with learners:

Staff will mute/disable learners' videos and microphones.

If only 1 student turns up and there is only 1 staff member the staff member will terminate the lesson and inform the DLP.

Prearranged Live 1:1 Sessions

Live 1:1 session will only take place with approval from the principal or the SEN Coordinator.

Live 1:1 session with learners are not recommended unless they are approved by the principal or the SEN Coordinator and a parent/carer is present in the room if possible (however, this may not be appropriate if providing counselling or safeguarding support). Where possible an SNA will be scheduled to "sit in" in a remote 1:1 lesson.

The following is the agreed protocol for 1:1 counselling provided by the two trained Guidance Counsellors in our school.

Support will be provided in line with

<https://www.education.ie/en/Schools-Colleges/Information/Post-Primary-School-Policies/continuity-of-guidance-counsellinghttps://www.education.ie/en/Schools-Colleges/Information/Post-Primary-School-Policies/continuity-of-guidance-counselling-guidelines-for-schools-providing-online-support-for-students.pdfguidelines-for-schools-providing-online-support-for-students.pdf>

The Guidance counsellors will agree with the principal/DLP the provisions to be in place and will follow best practice as laid down by the NCGE and the DES.

For further information on this please see the Whole School Guidance Plan.

Access links to live sessions should not be made public or shared by participants.

Learners and/or parents/guardians should not forward or share access links.

If learners/parents/guardians believe a link should be shared with others, they will discuss this with the members of staff running the session first.

Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

Alternative approaches and/or access will be provided to those who do not have access.

Behaviour Expectations

Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom. Students should note that the full code of behaviour continues to apply in a remote learning environment.

All participants are expected to behave in line with existing school/setting policies and expectations. This includes:

- Appropriate language will be used by all attendees.
- Staff or students will not take or record images for their own personal use.
- Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.

When sharing videos and/or live streaming, participants are required to:

- Wear appropriate clothes.
- Ensure backgrounds of videos are neutral (blurred if possible).
- Ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
- Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

Participants are encouraged to report concerns during remote and/or live streamed sessions:

- If students have any concerns, they should report them to the member of staff running the session or tell their parent/guardian.
- If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to the year head/Dean of Discipline.
- Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.

- Deliberate misuse of online platforms will be treated as a major or extreme breach of the code of behaviour.
- Any safeguarding concerns will be reported to Damien Kennedy DLP in line with the safeguarding statement.

Artificial Intelligence (AI) Use in School

Artificial Intelligence (AI) tools, such as chatbots, image generators, and translation software, are becoming part of everyday life. Used properly, they can support learning, creativity, and efficiency. This section sets out how AI may be used responsibly in our school.

1. Educational Purpose

- AI may only be used for school-related learning and teaching tasks, under the guidance of teachers or staff.
- AI is a support tool, not a replacement for your own ideas, effort, or critical thinking.

2. Responsible Use

- Always check and verify information from AI with trusted sources, as it may be inaccurate or biased.
- When AI is used to help with research, homework, or assignments, you must acknowledge it (e.g. "AI tool used to generate draft ideas").
- Do not use AI to complete work on your behalf in tests, exams, or assessments.

3. Respect and Ethics

- AI must never be used to create harmful, offensive, or inappropriate material.
- It is not allowed to use AI to impersonate others, create false information, or produce images, videos, or messages that could damage someone's reputation.
- Copyright rules apply — AI outputs must not be used to copy or misuse the work of others.

4. Privacy and Safety

- Do not share personal or sensitive information (your own or anyone else's) with AI systems.
- AI use must comply with data protection laws and the school's Data Protection Policy.

5. Staff Guidance

- Teachers and staff will guide students on the safe and appropriate use of AI in classwork.
- Staff are encouraged to model responsible AI use in their teaching and professional tasks.

6. Monitoring and Consequences

- The school may monitor AI use on school devices and networks.
- Misuse of AI (including plagiarism, unsafe behaviour, or harmful content) will be treated as a breach of this policy and may result in loss of access or disciplinary action.

For further information and links to Oide training, please see **Guidance on AI** from Department of Education and Youth:

https://assets.gov.ie/static/documents/dee23cad/Guidance_on_Artificial_Intelligence_in_Schools_2025.pdf

Personal Devices

Please refer to the mobile phone policy in relation to the use of mobile phones in the school setting.

All devices referred to in this policy are devices purchased under the following conditions:

1. Lenovo devices as identified in 1st year parent information evenings or other induction meetings, including, meetings with parents of students who enroll “mid-year” only.
2. Exchange students enrolled in the school, by agencies, and who are not staying any longer than one year may utilize their own devices.

Digital Learning Platforms (including video conferencing)

Nenagh College digital learning platform is owned and managed by the school. This platform should enable two-way communication.

Students must only use their school email to access the school’s digital learning platform.

All school-related media and data should be stored on the school’s platform.

The use of digital platforms should be used in line with considerations set out in the school’s data protection plan (GDPR).

Each user of the platform will be provided with their own unique login credentials.

Passwords for digital platforms and accounts should not be shared.

Personal email addresses should not be used when creating accounts on school digital platforms.

Images and Video

Care should be taken when taking photographic or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

At Nenagh College students must not take, use, share, publish or distribute images of others without their permission.

Taking photos or videos on school grounds or when participating in school activities is only allowed with expressed permission from staff.

Students must not share images, videos or other content online with the intention to harm another member of the school community.

Sharing explicit images and in particular explicit images of students and/or minors is unacceptable and absolutely prohibited behaviour. Sanctions, in accordance with the School's Code of Positive Behaviour will apply in these circumstances.

Inappropriate Activities

- Promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation.
- Misuse and fraud legislation.
- Racist material.
- Pornography.
- Promotion of any kind of discrimination.
- Promotion of racial or religious hatred.
- Harmful content or threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.
- Using school systems to run a private business.
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicizing confidential or proprietary information (e.g. financial / personal information, databases, computer / network access (codes and passwords)
- Creating or propagating computer viruses or other harmful files.
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet.
- Online gaming.
- Online gambling.
- Online shopping.
- Use of social networking sites, instant messaging and online forums.
- Child sexual abuse material.
- Any other activity that is considered questionable.

School Websites

Students will be given the opportunity to publish projects, artwork or schoolwork on the internet in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website.

Students will continue to own the copyright on any work published.

The website will be regularly checked to ensure that there is no content that compromises the safety, privacy, or reputation of students or staff.

Webpages allowing comments or user-generated content will be pre-moderated and checked frequently to ensure that they do not contain any inappropriate or offensive content.

The publication of student work will be coordinated by a teacher.

Personal student information including home address and contact details will not be published on Nenagh College web pages.

The school will ensure that the image files are appropriately named and will not use students' names in image file names or ALT tags if published online.

Cyberbullying

This type of bullying is increasingly common and is continuously evolving. It is bullying carried out using information and communication technologies such as text, social media, e-mail, messaging, apps, gaming sites, chatrooms and other online technologies. Being the target of inappropriate or hurtful messages is the most common form of online bullying. As cyberbullying uses technology to perpetrate bullying behaviour and does not require face to face contact, cyber-bullying can occur at any time (day or night). Many forms of bullying can be facilitated through cyber-bullying. For example, a target may be sent homophobic text messages or pictures may be posted with negative comments about a person's sexuality, appearance etc.

Access to technology means that cyberbullying can happen around the clock and the students' home may not even be a safe haven from such bullying. Students are increasingly communicating in ways that are often unknown to adults and free from supervision. The nature of these technologies means digital content can be shared and seen by a very wide audience almost instantly and is almost impossible to delete permanently. While cyberbullying often takes place at home and at night, the impact can also be felt in school.

In accordance with the Bi Cineálta Policy 2025, Nenagh College considers that a once-off offensive or hurtful public message, image or statement on a social network site or other public forum where that message, image or statement can be viewed and/or repeated by other people will be regarded as bullying behaviour.

When using the internet students, parents and staff are expected to always treat others with respect.

Engaging in online activities with the intention of harming, harassing, or embarrassing another student or member of staff is unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved.

Measures are taken by Nenagh College to ensure that staff and students are aware that bullying is defined as unwanted negative behaviour, verbal, psychological or physical, conducted by an individual or group against another person (or persons) and which is repeated over time. This definition includes cyberbullying even when it happens outside the school or at night. In addition, the Department of Education Anti-Bullying Procedures, 2013 defines cyberbullying as “placing a once-off offensive or hurtful public message, image or statement on a social network site or another public forum where that message, image or statement can be viewed and/or repeated by other people will be regarded as bullying behaviour.

The prevention of cyberbullying is an integral part of the Bi Cineálta Policy 2025 of our school.

Legislation

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

- Data Protection Acts 1988 to 2018 and General Data Protection Regulations (GDPR)
- Copyright and Related Rights Act 2000
- Child Trafficking and Pornography Act 1998 and Criminal Law (Sexual Offences) Act 2017
- Children First Act 2015
- Harassment, Harmful Communications and Related Offences Act 2020 (Coco’s Law)
- Criminal Damage Act 1991

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions

Misuse of the Internet and digital technologies are referred to in the school's Code of Positive Behaviour, Phone Use and Social Media Policy, and Bí Cineálta Policy and related sanctions regarding misuse as appropriate are outlined therein. The school also reserves the right to report any illegal activities to the appropriate authorities, including An Garda Síochána.

APPENDIX 1

AUP TO BE FOLLOWED IN EVENT OF REMOTE LEARNING

Remote learning will only take place using the Microsoft platform – Microsoft Teams, Microsoft OneNote, Microsoft Outlook, and Microsoft OneDrive.

Staff will only use their school assigned Microsoft Outlook Emails via Microsoft Teams to communicate with student school assigned profiles.

Use of any personal accounts to communicate with learners and/or parents/guardians is not permitted.

Students must use school emails only. Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the principal, the DLP.

Staff will work with equipment provided where possible, e.g. school provided Desktop, Laptop, iPad or other mobile devices. Staff will use strong passwords and log out of devices when not in use. If using devices other than one provided by teachers to inform the principal as he will need to communicate clear expectations regarding safeguarding and data security when using personal devices e.g., using strong passwords, suitable levels of encryption, logging off or locking devices when not in use etc.

Online contact with learners and/or parents/guardians will not take place outside of the operating times of the school day 8.45am – 3.30pm.

All remote lessons will follow the normal timetable.