



BANDONBRIDGE N.S.

Internet Acceptable Use Policy

Safe • Responsible • Respectful • Educational

Policy area	Digital learning, online safety and responsible technology use
Ratified by Board of Management	18 November 2024
Current revision	2026
Next review	Annually, or earlier where legislation/guidance requires

This policy should be read alongside the school's Code of Behaviour, Bí Cineálta Policy, Child Safeguarding Statement and Risk Assessment, Data Protection Policy, Digital Learning Plan and relevant school policies.

1. General Approach

The aim of this Acceptable Use Policy (AUP) is to ensure that pupils benefit from the learning opportunities offered by the school's digital resources in a safe, responsible, respectful and effective manner. Responsible use of the Internet, digital technologies and online services is an integral part of teaching and learning in Bandonbridge N.S.

Digital technologies change rapidly. This policy therefore applies not only to technologies specifically named in it, but also to comparable or emerging technologies used for school-related purposes.

When using the Internet and digital technologies, pupils, parents/guardians, staff and other members of the school community are expected to:

- treat others with respect and communicate in a courteous and responsible manner;
- protect their own privacy and the privacy, dignity and personal information of others;
- respect copyright, intellectual property and the work of creators;
- use school systems, accounts and devices only for authorised purposes;
- follow teacher/staff instructions and school safeguarding procedures;
- avoid actions that could compromise the security of school systems or bring the school into disrepute; and
- report online content, contact or behaviour that causes concern or makes them feel unsafe.

2. Scope and Responsibilities

This policy applies to:

- pupils who access the Internet, school devices, school accounts or digital services in Bandonbridge N.S.;
- staff, substitute staff, SNAs, volunteers, visitors and other authorised users of school systems;
- parents/guardians and carers where they access or use school-provided digital systems or communications; and
- school-related digital activity undertaken on or off the school premises where it has a connection with school life, school systems, the wellbeing of members of the school community, or the school's responsibilities under law and policy.

Parents/guardians remain responsible for supervising their children's use of personal devices, social media, gaming and Internet services outside school. The school is not expected to investigate every incident that occurs outside its care or responsibility. However, where online behaviour outside school has an impact in school, the school will support the pupils involved and, where the behaviour continues or otherwise falls within school procedures, will respond in accordance with the Bí Cineálta Policy, Code of Behaviour, Child Safeguarding Procedures and other relevant policies.

3. Promoting Safe and Responsible Use

- Internet safety and digital citizenship will be addressed through SPHE, Wellbeing, Digital Learning and other appropriate curriculum areas.
- Pupils will be taught age-appropriate strategies for privacy, passwords, respectful communication, recognising harmful or misleading content, reporting concerns, copyright and responsible use of AI.
- Internet safety advice and support may be provided through school programmes, visiting speakers and trusted online-safety resources.
- Staff will be encouraged to engage in continuing professional learning in online safety, data protection, digital learning and emerging technologies.
- Bandonbridge N.S. will participate in Safer Internet Day and other appropriate awareness initiatives.
- New apps, platforms and digital tools will be considered for educational value, age appropriateness, safeguarding, privacy, data protection and security before use.

4. Content Filtering and Network Security

The school will use appropriate technical and organisational measures to reduce online risk, including:

- content filtering provided through the Schools Broadband Network at the level selected by the school;
- supervised pupil Internet use;
- up-to-date security and virus/malware protection where appropriate;
- controlled installation of software and applications;
- secure passwords and individual accounts where appropriate;
- restrictions on unauthorised external storage media, software and network changes; and
- monitoring for unusual activity, security incidents and network-management purposes where lawful and proportionate.

Users must not attempt to bypass filtering, security controls, device-management settings or access restrictions by using proxy sites, VPNs, alternative accounts or other methods. Such behaviour may lead to withdrawal of privileges and other sanctions under school policy.

5. Internet Use

- Pupils will use the Internet for educational purposes and under staff direction.
- Pupils will not intentionally access material that is illegal, obscene, hateful, discriminatory, threatening, sexually explicit, violent, harmful or otherwise unsuitable.
- Accidental access to unsuitable material should be reported to a teacher immediately. A pupil who reports accidental access in good faith will be supported.
- Pupils will not plagiarise. Sources, including AI-generated material where permitted, must be acknowledged appropriately.
- Pupils will not disclose passwords, home addresses, telephone numbers or other unnecessary personal information online.
- Pupils will not download, upload or install non-approved files, applications or software.
- File sharing may be used with staff permission. Torrent sites and other unauthorised peer-to-peer services are prohibited.
- Users must not deliberately create excessive network traffic or interfere with another person's access to school systems.
- School Internet and digital-platform use may be monitored for safeguarding, security, technical and network-management purposes in accordance with law and school policy.

6. Email and Messaging

- Pupils will use only school-approved email or messaging accounts where these are provided for educational purposes.
- School accounts must not be used to register for unauthorised social networking services, games or apps.
- Passwords and login credentials must not be shared.
- Pupil email or messaging will be used under teacher supervision or with teacher permission as appropriate.
- Pupils must not send, request, forward or distribute content that is illegal, abusive, discriminatory, threatening, sexually explicit, defamatory or intended to harm, frighten, embarrass or intimidate another person.
- Any message or contact that makes a pupil uncomfortable or unsafe should be reported immediately to a trusted adult and should not be answered.
- Suspicious links, attachments and messages should not be opened without checking with a teacher.
- Pupils must not reveal unnecessary personal details about themselves or others.
- Pupils must never arrange to meet a person whom they know only through online communication.
- Attachments, forwarding, screenshots and 'reply all' should be used only where appropriate and, for pupils, with teacher permission.

7. Social Media and Messaging Services

Social media and messaging services can support communication but can also create risks relating to privacy, safeguarding, reputation and harmful behaviour. This policy applies to social networks, messaging apps, blogs, forums, livestreaming, video-sharing services, collaborative platforms and comparable services.

- Personal social media and instant-messaging services are not permitted for pupil use in school unless specifically authorised for an educational purpose.
- Staff may use school-approved platforms and accounts for school-related communication in accordance with school procedures.
- Members of the school community must not use digital services to harass, impersonate, insult, abuse, threaten, defame or deliberately embarrass another person.
- Personal or confidential information about pupils, staff or families must not be discussed or shared inappropriately online.
- School email addresses must not be used to create unauthorised personal social-media accounts.
- Personal views must not be presented as the views of Bandonbridge N.S.
- Staff should maintain appropriate professional boundaries in electronic communication and social media use.

8. Personal Devices and Assistive Technology

Pupils using approved assistive technology are expected to follow this AUP in the same way as when using school-owned equipment. The school's Home Use of Assistive Technology Policy should also be consulted where applicable.

- Pupils may bring personal Internet-enabled devices to school only with the express permission of the Principal or where specifically authorised under school procedures.
- Where a smartwatch is permitted, Internet, camera, messaging and recording functions must be disabled unless specifically authorised.
- Unauthorised photography, video or audio recording on personal devices is prohibited.
- Staff use of personal devices for school activities must comply with school data-protection, safeguarding and device-use procedures. Personal devices should not be used to store pupil personal data or school-related media unless specifically authorised and appropriately secured.

9. Digital Learning Platforms and Remote Learning

- School-approved digital learning platforms are managed or authorised by Bandonbridge N.S. and are to be used for educational and school-related purposes.
- Users will use unique login credentials where provided and must keep passwords secure.
- Personal email addresses should not be used to create pupil accounts on school platforms unless specifically approved and necessary.
- School-related media and pupil data should be captured, stored and shared only through school-approved devices, accounts and platforms, subject to school data-protection procedures.
- Where remote learning becomes necessary, the school may use an approved platform such as Microsoft Teams, Seesaw, ClassDojo or another service assessed and approved by the school.
- Online lessons and video conferencing must be conducted in a manner consistent with safeguarding, privacy, professional boundaries and school behaviour expectations.

10. Images, Audio and Video

- Images, audio and video involving pupils will be created and used only for legitimate educational or school purposes and in accordance with data-protection and safeguarding requirements.
- Pupils must not take, use, alter, share, publish or distribute images, audio or video of others without permission.

- Photography, video or audio recording on school grounds or during school activities requires staff permission.
- The school will obtain and manage parent/guardian permissions for publication of pupil images or work in accordance with its data-protection procedures.
- Personal pupil information such as home addresses, private contact details or other unnecessary identifying information will not be published.
- Content must never be created or shared with the intention of humiliating, threatening, sexualising, harming or exploiting another person.
- Creating, requesting, possessing, sharing or distributing sexual or sexually explicit images of children is strictly prohibited and may require safeguarding and/or statutory reporting.

11. Inappropriate and Prohibited Activities

The following are prohibited when using school systems or in connection with school-related digital activity:

- illegal activity, including offences relating to child sexual abuse material, harassment, harmful communications, unauthorised access to information systems, fraud or criminal damage;
- racist, discriminatory, hateful, pornographic, sexually explicit, threatening or seriously harmful content;
- cyberbullying, harassment, impersonation, intimidation or deliberate humiliation;
- bypassing filtering, security, account or device-management safeguards;
- unauthorised access to accounts, files, devices, networks or data;
- uploading, downloading or distributing copyrighted material without appropriate permission or licence;
- revealing confidential, personal, financial, proprietary or security information;
- online gambling, unauthorised shopping, unauthorised gaming or running a private business through school systems;
- use of age-inappropriate apps, services or games;
- using another person's account or attempting to obtain another person's password;
- creating or sharing deepfakes, manipulated media or AI-generated material intended to deceive, exploit, bully or harm; and
- any other activity that is unsafe, unlawful, seriously inappropriate or contrary to the ethos and policies of Bandonbridge N.S.

12. School Website and Online Publishing

- Pupils may publish schoolwork, projects or artwork through the school website and its blogs only with teacher permission and supervision.
- Pupils retain copyright in their original work, subject to applicable law and any permissions granted for school publication.
- School online content will be reviewed periodically to reduce risks to pupil and staff safety, privacy and reputation.
- Where practicable, group photographs and activity-based images will be preferred. Individual pupil content will be published only in accordance with school permissions and data-protection procedures.
- Full pupil contact details will never be published on school webpages or public-facing platforms.

13. Cyberbullying and Online Harm

Bandonbridge N.S. recognises that bullying behaviour may occur online or offline. In accordance with the Bí Cineálta Procedures, bullying is targeted behaviour, online or offline, that causes harm; the harm may be physical, social and/or emotional. Bullying behaviour is generally repeated over time and involves an

imbalance of power. A single harmful online message, image or video may constitute bullying behaviour where it is highly likely to be reposted or shared.

Cyberbullying may involve messages, social media, email, gaming, images, video, group chats, impersonation, exclusion, altered media or other digital technologies. Online content can be rapidly copied and shared and may have a continuing impact in school even when originally posted outside school.

- All members of the school community are expected to treat others with respect online.
- Online activity intended to harm, harass, frighten, shame or embarrass a pupil or staff member is prohibited.
- Where bullying behaviour occurs when pupils are not under the care or responsibility of the school, the school is not expected to deal with the out-of-school behaviour itself; however, where it has an impact in school, the school will support the pupils involved.
- Where bullying behaviour continues in school, or otherwise comes within the school's responsibility, it will be addressed in accordance with the school's Bí Cineálta Policy.
- Where an online incident raises a child-protection concern, the school will follow the Child Protection Procedures for Schools and Children First requirements.

14. Artificial Intelligence and Generative AI

Bandonbridge N.S. recognises that artificial intelligence (AI), including generative AI, may have educational value when used in an age-appropriate, transparent, safe and teacher-directed manner. AI does not replace teacher professional judgement, pupil effort, reliable sources or appropriate assessment.

- Only AI tools approved or authorised by the school/teacher may be used for school activities.
- Pupils must not use AI to complete homework, assignments or assessed work unless the teacher has explicitly permitted its use.
- AI-generated text, images, audio, video or other material must not be presented as a pupil's own original work. Where AI use is permitted, it should be acknowledged in a manner appropriate to the pupil's age and the task.
- AI output must be checked critically. Pupils should verify important information using reliable sources and should be taught that AI can produce inaccurate, biased, fabricated or inappropriate material.
- Personal, sensitive, confidential or identifying information about pupils, families, staff or the school must not be entered into public or unauthorised AI systems.
- AI must not be used to create harmful, sexual, discriminatory, defamatory, deceptive or bullying content, or to impersonate another person.
- AI-generated or manipulated images, audio or video must not be used to misrepresent another member of the school community.
- Before a new AI tool is introduced, the school will consider educational purpose, age requirements, privacy, data processing, security, safeguarding, transparency and any relevant terms of service.
- Staff should exercise professional judgement when using AI and should not rely solely on AI for decisions about pupils, assessment, safeguarding, behaviour, additional needs or other significant matters.
- Staff and pupils will be supported to develop AI literacy, including source checking, data literacy, bias awareness, copyright awareness and responsible prompting.

15. Data Protection, Privacy and Confidentiality

Personal data processed through school devices, platforms, websites, apps and digital services will be handled in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR), the Data Protection Act 2018 and the school's Data Protection Policy.

- Only the minimum personal data necessary for a legitimate school purpose should be collected, accessed, shared or stored.

- School accounts, platforms and devices should be used in a way that protects confidentiality and prevents unauthorised disclosure.
- Passwords must be kept secure and should not be shared.
- Pupil information, images, assessment information, special category data or other confidential information must not be uploaded to unauthorised services, including public AI tools.
- New digital services should be assessed for privacy and data-protection implications before use. Where required, the school will undertake appropriate risk assessment and/or a Data Protection Impact Assessment.
- Data breaches, lost devices, compromised accounts or accidental disclosures must be reported promptly to the Principal or designated person in accordance with school procedures.

16. Child Safeguarding and Online Safety

Online safety is part of the school's wider safeguarding responsibilities. Bandonbridge N.S. will respond to concerns about online grooming, sexual exploitation, child sexual abuse material, coercion, threats, harmful sexual behaviour, inappropriate contact or other child-protection concerns in accordance with the Children First Act 2015, Children First: National Guidance and the Child Protection Procedures for Schools 2025, as applicable.

Any member of staff who becomes aware of an online incident that may constitute a child-protection concern must follow the school's Child Safeguarding Statement and reporting procedures. Digital evidence should not be unnecessarily copied, forwarded or circulated.

17. Monitoring, Reporting and Sanctions

The school may monitor the implementation and impact of this policy through appropriate means, including:

- logs of reported incidents and actions taken;
- relevant pupil records in accordance with school procedures;
- network/security monitoring data;
- feedback, surveys or questionnaires from pupils, parents/guardians and staff; and
- review of emerging online-safety, safeguarding and digital-learning risks.

Serious online-safety incidents should be reported promptly to the Principal or, in her absence, the Deputy Principal. Where there is a child-protection concern, the school's child safeguarding procedures take precedence.

Misuse may result in consequences under the school's Code of Behaviour, Bí Cineálta Policy and other relevant policies. Depending on the nature and seriousness of the incident, consequences may include a warning, restricted or withdrawn digital privileges, restorative or educational responses, contact with parents/guardians, disciplinary action, or referral to relevant authorities. The school reserves the right to report suspected illegal activity to An Garda Síochána or another appropriate statutory body.

18. Review and Implementation

This policy will be reviewed at least annually, and earlier where necessary because of changes in legislation, Department guidance, technology, school systems or identified risk. Review may involve the Board of Management, teaching and support staff, pupils, parents/guardians and the Parents Association.

The school will monitor implementation through its established management and policy-review structures.

Appendix 1: Legislation and Guidance

This policy has been developed having regard to relevant Irish and European legislation and current school guidance. The following list is not exhaustive and should be read as including subsequent amendments, regulations and replacement guidance where applicable.

- General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018, together with relevant retained provisions of earlier data-protection legislation;
- Copyright and Related Rights Act 2000, as amended;
- Child Trafficking and Pornography Act 1998, as amended, including relevant provisions of the Criminal Law (Sexual Offences) Act 2017;
- Children First Act 2015;
- Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law);
- Criminal Justice (Offences Relating to Information Systems) Act 2017;
- Criminal Damage Act 1991, as amended;
- Children First: National Guidance for the Protection and Welfare of Children;
- Child Protection Procedures for Schools 2025;
- Department of Education Bí Cineálta Procedures to Prevent and Address Bullying Behaviour for Primary and Post-Primary Schools;
- Data Protection Commission guidance for schools, including the Data Protection Toolkit for Schools; and
- relevant Department of Education, Oide, Webwise, National Centre for Technology in Education/Schools Broadband Network and Teaching Council guidance, as updated from time to time.

Parent/Guardian Permission and Acknowledgement Form

As the parent/legal guardian of a pupil in Bandonbridge N.S., I confirm that I have read, or have had explained to me, the school's Internet Acceptable Use Policy. I understand that Internet and digital technology access is provided for educational purposes and that pupils are expected to use school devices, accounts, platforms and online services responsibly.

I understand that the school takes reasonable technical, educational and organisational measures to promote online safety, but that no filtering or supervision system can guarantee that unsuitable content will never be encountered.

I understand that my child's schoolwork and/or image may be published only in accordance with the school's data-protection procedures, permissions and this AUP. I understand that personal contact information will not be published.

Pupil name: _____

Class: _____

Parent/Guardian name: _____

Signature: _____

Date: _____

Appendix 2: Pupils in 3rd–6th Class

Bandonbridge N.S. Rules for Responsible Internet and Digital Technology Use

Our school has computers, laptops, iPads and other digital tools to help us learn. These rules help us to learn safely, protect ourselves and others, and use technology responsibly.

Internet and School Devices

1. I will use the Internet and school devices for learning and only when I have permission.
2. I will follow my teacher's instructions when using websites, apps, accounts and digital tools.
3. If I accidentally see something unsuitable, upsetting or strange, I will tell my teacher or another trusted adult straight away.
4. I understand that the school may monitor school devices, files and Internet use for safety and security.
5. I will not give out my home address, telephone number, passwords or other private information online.
6. I will not upload, download or install material unless my teacher has allowed it.
7. I will take care of school devices and will not change settings or try to bypass filters or security.

Email, Social Media and Messaging

8. I will not access my personal social-media, gaming or messaging accounts in school unless a teacher has specifically authorised an activity.
9. If my teacher gives me a school email or account, I will use it only for school purposes.
10. I will use kind, respectful and sensible language online.
11. I will not share photos, videos, screenshots or messages about other people without permission.
12. I will not arrange to meet someone I know only through the Internet, gaming or messaging.
13. I will tell a trusted adult if someone online makes me feel worried, uncomfortable, frightened or pressured.
14. I will not use technology to hurt, embarrass, threaten, exclude or frighten another person.
15. I understand that many social-media and messaging services have minimum-age rules and that I must follow school rules when I am in school.

Personal Devices

16. I understand that personal Internet-enabled devices are not allowed in school unless the Principal or school has given permission.
17. If I am permitted to wear a smartwatch, I will keep Internet, camera, messaging and recording functions disabled unless a teacher tells me otherwise.

Artificial Intelligence

18. I will use AI for schoolwork only when my teacher gives permission.
19. I will not pretend that AI-generated work is my own. I will acknowledge AI use when my teacher asks me to.
20. I will check AI answers because AI can make mistakes or invent information.
21. I will never put my own or another person's private, personal or confidential information into an AI tool.
22. I will not use AI to make fake, harmful, embarrassing, sexual, threatening or bullying pictures, videos, audio or messages about anyone.

My Agreement

I agree to follow Bandonbridge N.S.'s Acceptable Use Policy. I will use the Internet and digital technology responsibly, respectfully and safely. I understand that if I do not follow these rules, my digital privileges may be restricted or withdrawn and other school procedures may apply.

Pupil's name: _____

Pupil's signature: _____

Class: _____

Date: _____