Ennis National School

Acceptable Use Policy

Ennis National School
Ashline, Ennis, Co. Clare V95DE44
School Roll Number: 15042A
Phone: 065 682 9158
Website: www.ennisns.ie
Email: info@ennisns.ie principal@ennisns.ie

This policy has been formulated by Ennis National School whole-school Community and informs Staff and Parents of our Acceptable Use Policy.

1. Introduction

Ennis National School (ENS) acknowledges that access to the Internet and ICT provides valuable opportunities for our pupils and staff to learn, engage, communicate, and develop skills that will benefit them in many areas of their lives. However, like the real world, the Internet can expose children to unsuitable people and information, potentially impacting their attitudes, behaviour and well-being. Therefore, it is crucial to equip our pupils with the knowledge and skills necessary to navigate the Internet safely.

This policy applies to all "internet-enabled devices" including - but not limited to - computers, Chromebooks, iPads, laptops, smartphones, smartwatches, and other IT resources connected to the internet. It also covers device use (whether school-owned or personal) during school activities or transportation to and from these activities.

In addition, this policy applies to any behaviours that impact on ENS and members of the whole school community. Any action that causes harm to another member of the school community or that tarnishes the reputation of the school will be considered a direct breach of the school's Acceptable Use Policy (AUP).

This policy applies to staff, pupils and the whole school community of ENS. The school retains the discretion to modify this policy periodically. It should be carefully reviewed to ensure understanding and acceptance of its contents.

2. Rationale

The purpose of this policy is to provide guidance and direction on the acceptable use of Internet & ICT for teaching, learning, and communication for all members of the school community in a safe and effective manner. Internet access is viewed as a valuable resource and privilege provided by the school. Failure to comply with the school's AUP will result in the withdrawal of this privilege and/or the implementation of other appropriate sanctions.

3. Aim

The Acceptable Usage Policy (AUP) is designed to:
- Ensure that pupils can take advantage of the educational opportunities provided by internet access in a secure and positive way.
- Seek to establish minimum standards and inform pupils and parents about the school's management and monitoring of its devices, equipment, and networks.
- Highlight that all school ICT equipment should be used responsibly, in accordance with school policies.

- Treat all users respectfully, recognizing the privacy rights of each member of the school community.
- Observe copyright laws and give proper credit to creators when using online resources and content.
- Prevent misuse of ICT resources in any way that could tarnish the school's reputation.

4. Responsibilities of staff

ENS's computers and networks must be used responsibly, ethically, and in accordance with the law. Management retains the right to monitor usage.

Employees will:
- Adhere to the guidelines outlined in this AUP.
- Oversee pupil ICT usage, documenting and reporting any misuse of devices as appropriate.
- Demonstrate and instruct on the ethical and appropriate use of technology within a school environment.
- Stay focused on the curriculum.

5. School Strategies

ENS will implement several strategies to maximise learning opportunities while minimising internet risks. These strategies include, but are not limited to:

- Central Filtering System: All school devices use a central filtering system via the School Broadband Programme to minimise exposure to inappropriate material and block unsuitable sites. School devices also have regularly updated antivirus software where applicable.
- Internet Safety Information: Staff, pupils, and parents/guardians will be notified about relevant webinars and resources on internet safety.
- Routine Online Safety Promotion: Online safety will be routinely promoted through Webwise, parent-teacher meetings, staff meetings/conferences, in-class lessons (in line with SPHE Curriculum, e.g. Stay Safe), Internet Safety Week, or guest speaker workshops in the area.
- Non-Approved Software: Uploading or downloading unapproved software on school devices is prohibited.
- Supervised Internet Use: A staff member will supervise pupil internet use on school devices as appropriate.
- Anti-Bullying Policy: This policy should be read in conjunction with the school's Anti-Bullying Policy. Posting a single offensive or hurtful message, image, or statement on social media or other public forums that can be viewed and/or shared by others will be considered as bullying. This may include liking or sharing posts or videos that negatively portray others.

- 'Netiquette' and Responsible Use: Pupils will practise good 'netiquette' (positive online behaviours) at all times and refrain from any actions that could tarnish the school's reputation or that of a member of the wider school community. They will also handle school devices safely and responsibly and follow all related rules.

6. Support structures and Education

ENS strives to have support structures that promote the appropriate use of Internet-enabled devices in school and ensure that staff, parents/guardians, and pupils feel supported.

- Support Resources: The school will inform pupils and parents/guardians about key support resources and organisations that handle illegal or harmful internet activities.
- Internet Safety Program: The school will regularly conduct a program on acceptable internet usage for pupils, covering topics like cyberbullying.
- Community Guard Partnership: ENS will coordinate with the community guard regarding internet safety and cyberbullying.
- Prohibited Social Media Conduct: Parents/guardians or visitors must not use social media or the internet to harass, insult, abuse, or defame pupils, their families, staff, or other members of the school community.
- Restrictions on Media Sharing: Parents/guardians or visitors should not upload images or videos of ENS pupils or staff to social media platforms, including those from school events like concerts and sports days.
- Avoid Bringing Disrepute: Parents/guardians or visitors must refrain from any social media or communications activity that could tarnish the reputation of ENS.
- Adhere to Age Requirements: Parents/guardians should ensure that their children meet the minimum age requirements for messaging services and social networks. Though the school will not monitor this, parents are advised not to allow their children to have personal accounts on platforms like Facebook, X (formerly Twitter), Tik-Tok, Snapchat etc, until they meet the legal age requirements.
- Monitor Child's ICT Use: Parents/guardians should monitor their children's use of ICT and electronic (including all internet-enabled) devices and be responsible for their online behaviour outside of school. While school authorities cannot be held responsible for off-campus online behaviour, the school will cooperate with parents/guardians to address inappropriate online incidents that affect the well-being of pupils or staff. Parents/guardians will be advised to report these incidents to the Gardaí.

7. Acceptable Use of the Internet for Pupils

- Online Safety Lessons: Teachers will deliver specific lessons on online safety (e.g., Webwise, Zeeko's 5 in 1 Rule, and All Aboard for DigiTown). Senior pupils receive internet safety talks from local Gardaí or professional organisations.
- Accessing Inappropriate Sites: Pupils will not intentionally attempt to access obscene, illegal, hateful, or otherwise objectionable websites on school devices. The school is not responsible for any attempts in this regard.
- If pupils accidentally access such sites, they are expected to inform a teacher immediately. pupils will report accidental accessing of inappropriate materials in school but outside the classroom to The Principal, Deputy Principal or Mr Gary Walsh (Digital Coordinator).
- Educational Internet Use: The internet will be used by pupils for educational purposes to enhance learning.
- Copyright and Fair Use: Pupils will not upload, download, or transmit copyrighted material on school devices.
- pupils will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- pupils 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.
- Personal Information: Pupils will not share their or others' personal or confidential information online, such as their or peers' addresses, phone numbers, email addresses, online profile data, images or school details.
- Account Privacy: Pupils will not examine, alter, or use another person's files, usernames, or passwords.
- Monitoring and Discipline: Pupils should be aware that any use of school devices, including sending or receiving personal or school-related information, may be monitored and subject to disciplinary action.
- Online Safety Responsibility: The school takes reasonable precautions to ensure online safety but cannot be held responsible if pupils deliberately or inadvertently access inappropriate sites.
- Email and Google Drive: Where provided, pupils will use approved school email accounts, Google Classroom and G-Suite Apps under teacher or parent/guardian supervision.
- Prohibited Email Conduct: Pupils will not download, send or receive illegal, obscene, defamatory, or harassing material.
- Meeting Online Contacts: Pupils will never arrange face-to-face meetings with individuals they know only through email or the internet.
- pupils taking steps to by-pass 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.
- pupils will never disclose or publicise personal information or passwords.
- Use of file sharing and torrent sites is allowed with staff permission.

8. Distance Learning

Online Teaching Guidelines:
- Platforms: When teaching cannot occur on-site, teachers may use Google Classroom, Class Dojo, and other approved platforms such as Padlet, Google Meet, Zoom, and SeeSaw (the "Online Platforms") for essential remote instruction as deemed appropriate.
- Terms of Service: The school has agreed to the terms of service for the Online Platforms used.
- Security & Privacy: The school has activated the latest security and privacy features provided by these platforms.
- Parental Monitoring: Parents/Guardians will receive the password and are expected to monitor their child's use of these Online Platforms.
- Consent for Virtual Lessons: For Google Meet, Zoom or other approved platform classes, parents/guardians must provide consent for their child's participation
- Parental Supervision: Parents/Guardians should supervise their child's participation on these platforms

Borrowing School Technology (Distance Learning):
Recognizing that some households lack necessary technology for distance learning, the school may lend suitable devices to pupils for educational use on a case-by-case basis. The following guidelines apply:
- The device remains the property of ENS
- Only the assigned pupil may use the device; it must not be tampered with, transferred to, or used by a third party.
- Parents/guardians and pupils are responsible for proper care and maintenance.
- The device must be returned in good condition with all components (e.g., charger, cover).
- Internet usage should be supervised by a parent/guardian and limited to appropriate content.

Internet Chat:
- Online chat will only be used for educational purposes under teacher guidance and parent/guardian supervision.
- pupils are prohibited from arranging face-to-face meetings with anyone they only know online. See web safety skills lessons like those on Webwise.
- Google Classroom/Zoom discussion forums are strictly for educational purposes and will always be supervised.

9. School Website, App (and affiliated Social Media sites)

- The school's website address is www.ennisns.ie
- The school uses the Aladdin Schools App (administrative tool which is known as *Aladdin*)
- The school's Twitter account is '*@ennisns*'.
- The school's Instagram account is '*@ennisns'*
- The 'Ennis National School Parents Information Page' is a Facebook page run by a parent, a school representative and a Parent's Association representative where all content and posts are filtered, pre approval is required before posts are allowed and rules of participation are displayed on the page.

- Pupil Work Publication: Pupils can have photos, projects, artwork, and other work related to curricular and extracurricular activities published on the school website or social media channels according to the consent form. Class teachers and/or the designated social media team of volunteering teachers will manage the publication of this material.
- Personal Information Exclusion: Personal information about pupils, such as their full name, home address, and contact details, will not be included on school social media or the school's website.
- Digital Media of pupils: Individual pupils' digital photographs and audio or video clips will not be posted on the school website or affiliated pages without prior parental/guardian permission.
- Event Media: Photos/videos may be used for specific school events (e.g., Confirmation, school tours, Sports Day). These photos/videos, including those on the school website/app, should not be copied or posted to social media or other websites.
- Social Media Tagging: Parents/guardians are requested not to tag photos or any content on social media that identifies children or staff from the school.
- Respectful Online Interaction: Parents/guardians are asked to ensure that online messages and comments on the school's social media sites remain respectful, as they are treated like written messages sent directly to the school.
- Reporting Concerns: If any parent or guardian has concerns about the website or social media content, the Board requests that they notify the school immediately.
- Policy Reference: This policy should be read in conjunction with the Data Protection Policy.

10. Use of Information Communication Technology ("ICT") Resources

- School Technology Resources: ENS's information and technology resources (e.g., email, computers, applications, networks, internet, intranet, phones, fax machines, printers and wireless communication devices like iPads, Chromebooks, laptops, telephones, pagers, and voicemail systems) are school property and intended solely for school-related activities.
- Prohibited Usage: Inappropriate use, including hacking, pirating software, using resources for non-school commercial activities, soliciting, distributing literature for external organisations, disclosing confidential school information, sending inappropriate emails, or accessing websites that promote hate, violence, or illegal activities, is forbidden. Misuse that violates school policies or tarnishes the school's reputation is also prohibited.
- Password Protection: Users must not share passwords. If a user allows others to access their password or assigned resource, they will be held responsible for any misuse.
- Monitoring and Disciplinary Actions: The Board of Management reserves the right to monitor the use of its information and technology resources. It may impose disciplinary measures or deny future access if misuse occurs.
- Consent to Monitoring (Pupils): Pupils' use of school technology resources implies consent to monitoring, which will be conducted in compliance with applicable laws, including the EU's General Data Protection Regulation (GDPR).
- Consent to Monitoring (Staff): Staff using school technology resources consent to monitoring in line with applicable laws, including GDPR.

Personal Devices:
- Ennis NS reserves the right to permit children to bring their personal devices to school where appropriate. Permission must be given by a teacher.
- Unless permission is given by a teacher, pupils are prohibited from using personal devices capable of recording or taking images during school hours, while on school grounds or while on school outings (including school tours, field trips and excursions). Violating the AUP will result in disciplinary action.
- Personal internet-enabled (or other electronic) devices found on a pupil during school hours will be confiscated and kept by the teacher in question, in the principal's office, or other secure office until a parent/guardian is contacted and collection is arranged.
- E-readers may be permitted with teacher supervision.
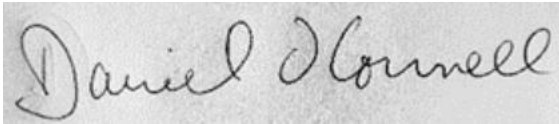- Assistive technology devices should only be used for educational purposes.

11.Sanctions

- Disciplinary Actions: Misuse of the internet or any activities that violate this policy may lead to disciplinary action. This could include written warnings, revoked access privileges, and, if warranted, suspension or expulsion in accordance with the Code of Behaviour.
- Reporting to Authorities: The school reserves the right to report any illegal activities to the relevant authorities.
- Withdrawal of Access: Pupils who do not uphold acceptable standards of internet use will have their access privileges revoked.

12. Review and Ratification

The school will conduct a regular review of this AUP policy and reserves the right to modify or revise its usage in accordance with school priorities.

The Board of Management ratified this AUP Policy on: 23rd September 2024

Signed:

Chairperson, Board of Management