Knocknacarra Educate Together National School

Internet Acceptable Use Policy

This policy has been formulated by Knocknacarra ETNS to provide guidance for staff members, pupils and any other individuals using internet-enabled devices at the school.

Contents

Introduction:

This policy on internet acceptable use was written in consultation with staff and the Parent-Teacher Association and approved by the Board of Management of Knocknacarra Educate Together NS, based on the original policy written in 2017 and reviewed in 2020 and 2024.

Background and Rationale:

Knocknacarra Educate Together NS believes technology is an important and valuable tool for learning and teaching. The school values its uses and believes it is important to equip pupils with the knowledge and skills to use the internet safely and with good judgement. This policy sets down procedures and guidelines for anyone using internet-enabled devices in the school environment.

Relationship to School Ethos:

Knocknacarra ETNS follows the key principles of Educate Together: equality-based, co-educational, child-centred and democratically run. The protection of pupils is paramount, and they must be enabled to use internet-enabled devices safely and responsibly as modelled by staff members.

Aims and Objectives:

- To identify when and how internet-enabled devices will be used in the learning context.
- To specify acceptable usage for both staff and pupils.
- To identify the protocols in place concerning the use of internet-enabled devices in the school.

Policies and Procedures:

Acceptable Usage for Pupils

The school currently has a set of tablets (30) and two sets of laptops (30 each) that are stored in portable charging trolleys. In addition, each classroom has an interactive board or projector connected to a teacher laptop. The following protocols will guide all use of internet-enabled devices:

1. Before students are allowed to use internet-enabled devices, all parents/guardians will be required to grant permission. This is done when pupils enrol for the first time in the school.
2. When pupils have access to the internet in school, it will be under the supervision of a staff member.
3. Whenever pupils are using a technology device, the purpose of the task will be clear, and any other use of the device beyond the task expectations will not be permitted.
4. Content will be subject to the restrictions of the automated web-filtering function. The purpose of content filtering is to ensure (in so far as possible) that inappropriate websites and content are not accessible from within the school.
5. Students will report accidental accessing of inappropriate materials.
6. Students will never disclose or publicise personal information about themselves or others.
7. Online tasks that involve sending and receiving email (e.g. with partner schools, educational email tasks) will be teacher-led. The class teacher will set up one email address for the class. Only the teacher will know the password to such email accounts. Emails will be opened and read by the teacher before being shared with the class. All emails will be reviewed by the teacher prior to sending. Students will write and read emails from the class email account only under the direct supervision of the teacher. Pupils will not have access to email passwords or administrator accounts.

8. Pupils will observe good "netiquette" (internet etiquette) at all times and will not undertake any actions that may bring the school into disrepute.
9. Uploading and downloading of non-approved software will not be permitted.
10. The use of students' personal pen drives, external drives, CD ROMs, and DVDs in school requires permission from the teacher.
11. Pupils will be given the opportunity to publish projects, artwork and schoolwork on the school website. For more information, see the Social Media and School Website Policy.
12. Pupils are not allowed to bring and/or use their own personal devices.
13. Pupils will experience developmentally appropriate discrete lessons on how to use the internet safely and what to do if they encounter inappropriate images or text. In addition, as part of the Anti-Bullying Policy, age-appropriate lessons regarding cyber-bullying will be taught.
14. In the event that pupils breach these protocols, the matter will be addressed according to the school's Code of Behaviour and may lead to a loss of privileges regarding the use of ICT devices.
15. On occasion, the school will loan a device to be used at home, either to support distance learning during exceptional closures or as ongoing assistive technology tool. All of the above expectations remain in place, and the device shall remain the property of the school. Parents and children take responsibility for the careful maintenance and proper usage of the device, including repair and replacement, if required. Parents must supervise internet usage on these devices at all times as the school's internet filtering is site-based. As much as possible, the settings will be child-friendly when the device is given to families, but the school cannot accept responsibility for supervising the internet access when a child uses the device. Parents will be given information in writing on how to use safety features from the website www.webwise.ie. Appendix A will be signed by the parent before taking a device from the school for use at home. When devices are returned, they will be cleaned, all files will be removed and all settings restored.

Distance Learning Platforms

1. During extended closures as well as to support ongoing learning, the school may use two platforms: Seesaw and Google Classroom.
2. Seesaw is an online platform is accessed through a unique code that is provided to parents when they grant permission for their child to engage with this platform. Two-way communication takes place between children, supported by parents, and teachers. Children and teachers may upload video and audio recordings. They may also share documents. If the blog aspect of the platform is used, it will remain password-protected rather than public. Class comments are currently disabled. Teachers may also share children's work with the class in the form of an assignment to be viewed without using the blog. Children and parents make the decision of which recordings and documents will be shared, and they can remove them independently, requesting assistance from the class teacher if required.
3. Children in 3rd Class and above use the GSuite for Education. Children are assigned a Google ID, which resembles an email. Passwords are set by the school. These logins may be used, as requested by the teaching staff, to access other online sites such as Khan Academy. The school administrator determines which GSuite functions are permitted. At present, Gmail is disabled. For distance learning, Google Classroom may be used but cannot be accessed without an invitation and solely using the school-assigned login details. Assignments are uploaded. Also, the Stream is used to promote dialogue and share learning among the class. Class comments are

allowed, and this is used to practice appropriate social media etiquette. They are closely monitored by class teachers. Children are also able to make private comments to the teacher.

4. On occasion, online assemblies and class meetings may take place using Google Meets or another similar platform approved by the principal. Links for meetings are never publicly shared. Children and staff have the option of being visible or having the camera turned off. All such meetings are voluntary for pupils. For younger children, supervision and support from an older person is required. Permission to participate in such events should be granted in advance. The recording of any such meeting by pupils and parents is disabled.
5. The guidelines in the school's Code of Behaviour and Anti-Bullying Policy apply in all online interactions. Here are a few key points to remember:
    - Be kind in every interaction, showing respect for teachers and fellow classmates at all times.
    - Be safe, ensuring that any videos uploaded are respectful (think about background noise, an appropriate setting, respectful clothing, etc.).
    - Be patient and ask for help as launch new platforms are launched.

Acceptable Use by Staff Members and Other Responsible Adults

1. If a teacher wishes to integrate a web page into a lesson, that page must be fully previewed/evaluated prior to its classroom usage, for inappropriate advertising content, imagery, and text. If such content exists on the webpage, teachers must download the required lesson content to a Word document and close the webpage prior to the lesson.
2. The installation of software, whether from CD-ROM or online sources, must be preapproved.
3. Staff members may not use their own devices with pupils.
4. Staff will observe good "netiquette" (internet etiquette) at all times and will not undertake any actions that may bring the school into disrepute.
5. Teachers may not use school devices for personal purposes. While teachers may take home devices with advanced permission from the principal, they may not be used for any reason other than for professional purposes.
6. Staff members are provided with email addresses. Users must not use the service for the transmission of illegal material. The user agrees to refrain from sending or receiving any materials deemed to be offensive, abusive, indecent, defamatory, obscene or menacing as prohibited by current and future statutes in force. The user agrees to refrain from sending or receiving material which may be in breach of copyright (including intellectual property rights), confidence, privacy, or other rights. Users must not participate in the sending of unsolicited or bulk email, commonly referred to as 'spam'. School email addresses are reserved solely for professional purposes.
7. Pupils' work should never be shared on social networking sites or websites other than the school website and Facebook page.
8. Users may not gain or attempt to gain unauthorised access to any computer for any purpose. In addition to being in breach of this AUP, such action may lead to criminal prosecution.
9. Users must not send data via the internet using forged addresses or data which is deliberately designed to adversely affect remote machines (including but not limited to denial of service, ping storm, Trojans, worms, and viruses).
10. Users are prohibited from running 'port scanning' or other software intended to probe, scan, test vulnerability of or access remote systems or networks except in circumstances where the remote user has given express permission for this to be done.

11. Users may not divulge their computer network passwords to third parties and must take all reasonable steps to ensure that such information remains confidential.
12. Access to the network may only be made using the authorised logon name and password.
13. Activity that threatens the integrity of the school's ICT systems or activity that attacks or corrupts other systems is forbidden. This includes browsing system files and changing any system settings.
14. Personal USB storage devices should be monitored for corruption and used with caution. In the event that a USB storage device is presenting signs of corruption or potential virus activity, it must no longer be used within the school's computer network. Additionally, while the school network is regularly swept for viruses and anti-virus software is used to prevent virus activity, the school accepts no responsibility for damage caused by computer viruses.
15. Other users' files must never be accessed.
16. In the interest of protecting the network from potential virus activity, the downloading of programs, games, screensavers, and wallpapers from the internet or uploading from a CD-ROM should be done carefully, and support from the principal should be sought as needed.
17. Use of the computing facilities for personal financial gain, gambling, political purposes, or advertising is forbidden.
18. In order to protect the information that is accessible on Aladdin, users must not divulge logon details to third parties. Any concerns or queries must be forwarded and dealt by the principal who has administrator rights on the Aladdin system.
19. Should a user share their own name, address, credit card or bank details or other personal information, it is done so at their own risk and the school accepts no responsibility.
20. The school operates a wireless network. Wifi is configured on wireless devices that students are permitted to use. To prevent unnecessary consumption of bandwidth, usage is limited to school devices. Given that all wireless devices will connect to the school's wireless network, they are subject to filtering under the Broadband for Schools Programme. Visitors to the school will require specific permission to use school devices, and this will be done strictly under the supervision of a staff member.
21. Staff members are encouraged to use the freeze function on the projector when doing searches on the interactive whiteboards.
22. Staff members are required contractually to adhere to this policy. Any violations of this policy will be addressed immediately and could lead to suspension or termination.

Support Structures

- The school will provide internet safety and cyber-bullying lessons at least biannually for pupils from 1st – 6th class as part of the Social, Personal and Health Education (SPHE) curriculum.
- The school will provide internet safety and cyber-bullying talks for parents and guardians on a regular basis.
- Community gardaí and other internet-safety trainers may visit classes regarding internet safety and cyber-bullying.
- Staff are encouraged to pursue continuous professional development opportunities in relation to internet safety and cyber-bullying.
- Staff will collaborate to train one another in effective and safe use of ICT equipment.

Implementation and Review:

The policy has immediate effect and will be reviewed no later than 2027.

Ratification and Communication:

The revised policy was ratified by the BoM on the date below. It will be posted on the school website.

Paul Adams, chairperson Date of ratification: 14/04/2024

Appendix A - Agreement for Use of School-Owned Technology Devices

Child's Name _____

Name of Parent(s)/Guardian(s) _____

Item(s) Being Loaned:

_____

_____

Date Item(s) to Be Returned: _____

In agreement with the Internet Acceptable Use Policy, Code of Behaviour and Child Safeguarding Statement of the school, I agree to all the requirements including:

- The device will be kept safe, and any malfunction or damage will be reported to the school.
- Parents are liable for replacement and/or repair of the device.
- The device will only be used for educational purposes and only by the children in question.
- No changes to the device, including the installation of unauthorised software and changes to system settings, will be made.
- Use of the internet will be closely monitored by parent(s)/guardian(s) in acknowledgement of the fact that the web filtering system in place in the school building does not function when a device is used in another setting. The school can accept no responsibility for the off-site use of the devices. Information on how to set up parental controls has been provided.

_____ _____

Signature(s) of Parent(s)/Guardian(s) Signature of School Representative

_____

Date