Scoil Mhuire gan Smál, Cill Choirle

Electronic Device Acceptable Use Policy

Policy Details

Name of Policy:	Administration of Medication Policy	
Date developed:	2009	Signed by
Date Reviewed:	Sept 2020	Chairperson: Geraldine Kirk
Ref Code:	TBA	Principal: Donna Kiby
Edition:	v1	Date commenced: 15/09/2020

1. Policy Statement

1.1. Scoil Mhuire gan Smál is committed to providing pupils with best opportunities to access internet resources in the context of their individual and overall learning whilst protecting the rights and confidentiality of all persons in the school.

1.2. This policy is to be read in conjunction with our Anti-bullying policy which includes cyberbullying.

2. Policy Purpose

2.1. This policy aims to provide school staff, parents and pupils with guidance on the safe and acceptable use of electronic devices in school.

2.2. The aim of this policy is to ensure that pupils will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.

3. Policy Scope

3.1. This policy applies to all teachers, school personnel, parents, pupils and other persons engaged in school activities.

4. Legislation

4.1. Scoil Mhuire gan Smál provides information to teachers and parents on relevant legislation relating to the use of internet, including:

- 4.1.1. Child trafficking and Pornography Act 1998
- 4.1.2. Interception Act 1993
- 4.1.3. Video Recordings Act 1998
- 4.1.4. The Data Protection Acts 1988-2018
- 4.1.5. GDPR

4.2. Information on this legislation can be found by following links on the school website.

5. General Principles

5.1. The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet.

5.2. Internet sessions are always supervised by a teacher. No student may have internet access unless agreed with the teacher and the teacher is present.

5.3. Filtering software and/or equivalent systems is used in order to minimise the risk of exposure to inappropriate material.

5.4. The school monitors pupils' Internet usage and search history.

5.5. Students and teachers are provided with training in the area of Internet safety.

5.6. Uploading and downloading of non-approved software is not permitted.
5.7. Virus protection software is used and updated on a regular basis.
5.8. The use of personal memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission.
5.9. Students must always treat others with respect while online and must not undertake any actions that may bring the school or themselves into disrepute.

6. World Wide Web

6.1. Students must use the Internet for educational purposes only.
6.2. Students must not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
6.3. Students must report accidental accessing of inappropriate materials to their class teacher who may then refer to the matter to the Digital Learning Team
6.4. Students must not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
6.5. Students must never disclose or publicise personal information.
6.6. Downloading materials or images not relevant to their studies, is in direct breach of the school's acceptable use policy.
6.7. Students are informed that any usage, including distributing or receiving information, school related or personal, will be monitored for unusual activity, security and/or network management reasons.

7. Email

7.1. Students must only use approved class email accounts under supervision by or permission from a teacher.
7.2. Students must not send or receive any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
7.3. Students must not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
7.4. Students must never arrange a face-to-face meeting with someone they only know through emails or the internet.
7.5. Students must note that sending and receiving email attachments is subject to permission from their teacher.
7.6. Parents and staff should only communicate through the official school email address (secretary@kilkerleyns.ie) or school email addresses provided by teachers, rather than teachers' personal email addresses.
7.7. Students may send homework to email accounts created by their teachers. These accounts are for this purpose only and are not to be used as a means of communication between school and home.

8. Internet Chat

8.1. Students only have access to chat rooms, discussion forums, messaging or other electronic communication that have been approved by the school, e.g. Skype, Seesaw
8.2. Chat rooms, discussion forums and other electronic communication forums must only be used for educational purposes and will always be supervised by the class teacher.

8.3. Usernames are used to avoid disclosure of identity.
8.4. Face-to-face meetings with someone organised via Internet chat is forbidden.

9. School Website: www.kilkerleyns.com

9.1. Pupils will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website. All such publication will be co-ordinated by a teacher.
9.2. The website is regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
9.3. Website using facilities such as guest books, notice boards or web blogs are checked frequently to ensure that they do not contain personal details.
9.4. The publication of student work will be coordinated by a teacher
9.5. Digital photographs, audio or video clips focusing on group activities and /or individual students will only be published on the school website with parental permission.
9.6. Personal pupil information including home address and contact details will be omitted from school web pages.
9.7. The school website will avoid publishing the first name and last name of pupils in a photograph.
9.8. The school will ensure that the image files are appropriately named and will not use pupils' names in image file names or ALT tags if published on the web.
9.9. Pupils will continue to own the copyright on any work published.

10. Scoil Mhuire gan Smál, Kilkerley Twitter account @KilkerleySchool

10.1. The purpose of having a school Twitter account is to provide communication with parents regarding specific events & activities.
10.2. This account is a closed account and therefore parents must apply to the school to be granted access.
10.3. Access to the account is withdrawn when these parents no longer have children in the school.

11. Personal Devices

11.1. Pupils are not permitted to bring personal electronic devices to school. However, pupils who have been assessed as requiring assistive technology will be permitted to use personal devices between home and school with the agreement of parents and class teacher.
11.2. Pupils who are permitted to use a personal device in school must have them password protected.
11.3. Where a pupil brings a personal device to school, the device must be kept in the office switched off during the school day and may not be used, for any purpose, on school premises, grounds or during off-site school activities (such as school

swimming or sports activities). The only exception to this is in an emergency or with the approval of a teacher. Such devices should be labelled clearly with the pupil's name.

11.4. Pupils who ignore this policy and use a personal device on school premises without permission will be required to hand over their device to a member of staff and parents will be asked to collect it from the school office.

11.5. Pupils using their own technology in school, such as leaving a device turned on or using it in class, sending nuisance text messages, or the unauthorized taking of images with a recording device, still or moving, is in direct breach of this policy.

11.6. The school accepts no responsibility for replacing lost, stolen or damaged personal devices that have not been handed up for safe keeping under the conditions outlined above. Nor does it accept responsibility for loss or damage sustained while travelling to and from school.

11.7. Pupils using personal devices to bully other pupils or send offensive messages will face disciplinary actions as per the School Code of Behaviour and the Anti Bullying Policy.

11.8. Where it is suspected that a pupil has made an inappropriate recording on a personal device, the teacher may request the pupil to hand over their device and seek to view the recording. Where necessary, the teacher may request a parent to be present when viewing this material. Where there is a suspicion that the material on the device may provide evidence relating to a criminal offence, the device will be handed over to the Gardaí, with the parents' knowledge, for further investigation.

11.9. It should be noted that it is a criminal offence to use an electronic device to menace, harass or offend another person. As such, if action as sanctioned by the school in this regard is deemed ineffective, as with all such incidents, the school may consider it appropriate to involve the Gardaí.

12. Inappropriate Activities

12.1. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: (*These activities are illegal in Ireland)

- Child sexual abuse images*
- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation*
- Racist material*
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- 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 publicising 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
- On-line gaming (with the exception of educational pre-approved online games found on our ICT Internet Resources folder)
- On-line gambling
- On-line shopping / commerce
- File sharing
- Use of social networking sites

13. Support Structures

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

13.2. https://zeeko.ie/

13.3. https://www.webwise.ie/

13.4. https://www.safefood.eu/Education/Primary-(ROI)/MediaWise.aspx

13.5. https://www.commonsensemedia.org/

13.6. https://cybersafeireland.org/

13.7. https://www.gov.ie/en/campaigns/be-safe-online/

13.8. https://kidshealth.org/en/parents/net-safety.html

13.9. http://www.schooldays.ie/articles/5-internet-safety-steps-parents-should-take

13.10. http://www.justice.ie/en/JELR/Pages/Cybercrime

13.11. Internet Safety talks for students and parents may be provided if needs be.

14. Sanctions

14.1. Misuse of electronic devices will result in disciplinary action, which may include written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion (see Anti Bullying Policy). The school also reserves the right to report any illegal activities to the appropriate authorities.

15.Development and Review

15.1. This policy was developed in 2009, reviewed in 2016, 2019 and September 2020.

15.2. This policy incorporates and will replace the previous "Mobile Phone Policy".

15.3. This version was reviewed by Parent representatives from the Parent's Association and the Board of Management.

15.4. This version was reviewed by the Principal, Staff and Digital Learning Committee.

15.5. This policy will be reviewed regularly in line with developing technological issues, and no longer than every three years.

Permission Form

Pupils
Please review the attached school Internet Acceptable Use Policy, sign and return this permission form to the Principal, Scoil Mhuire gan Smál, Kilkerley

Name of Pupil: _____

Class: _____

Pupil:
I agree to follow the school's Acceptable Use Policy on the use of the Internet. I will use the Internet in a responsible way and obey all the rules explained to me by the school.

Pupil's Signature: _____ Date: _____

Parent/Guardian:
As the parent or legal guardian of the above pupil, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access the Internet. I understand that Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if pupils access unsuitable websites.

Parent's/Guardian's Signature: _____ Date: _____

In relation to the school website, I accept that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing children's work on the school website.

Parent's/Guardian's Signature: _____ Date: _____

Address: _____ **Phone**: _____

_____

_____

Letter to Parents/Guardians

Dear Parent/Guardian,

Re: Internet Permission Form

As part of the school's education programme we offer pupils supervised access to the Internet. This allows students to access to a large array of online educational resources that we believe can greatly enhance the learning experience.
However, access to and use of the Internet requires responsibility on the part of the user and the school. These responsibilities are outlined in the school's Acceptable Use Policy (enclosed). It is important that this enclosed document is read carefully, signed by a student and parent/guardian and returned to the school.
Although the school takes active steps to promote safe use of the Internet, it recognises the possibility that students may accidentally or deliberately access inappropriate or objectionable material.
The school respects each family's right to decide whether or not to allow their children access to the Internet as defined by the school's Acceptable Use Policy.
Having read the terms of our school's Acceptable Use Policy, you may like to take a moment to consider how the Internet is used in your own home, and see if there is any way you could make it safer for your own family.

Yours sincerely,

_____

AUP checklist

For an AUP to be robust it needs to be reviewed and updated regularly taking into consideration implementation issues that may arise. The following is a checklist that may be used when developing or revising an AUP.

Have AUP implementation issues arisen since the AUP was designed/revised? ☐

Have these issues been discussed with parents, students and teachers and incorporated into an update UP? ☐

Given that an AUP is in place, can the school confidently address the following scenarios?

- A student is found using a chat room to arrange a face-to-face meeting with a friend ☐
- The school uses filtering software but a student accidentally accesses a pornographic website while in yo ☐ re
- A student publishes defamatory information on a personal website about a peer ☐

Has the AUP had a positive impact on curriculum delivery? ☐

Has internal or external expertise assisted the formulation or reformulation of the AUP? ☐

Has the AUP as a code of Internet use transferred to home use? ☐

Does an open dialogue exist between students and teachers relating to Internet misuse and safety issues? ☐

Are teachers' and students' internet safety training needs being met ☐