Internet Safety: Acceptable Use Policy

School Name: St Colman's National School

Address: Cummer, Corofin, Tuam, Co Galway

Overview

This Acceptable User Policy (AUP) is in two sections. Section A relates to the use of the internet by students within the school and personnel working on their behalf. Section B relates to staff and visitors to the school who are using the internet and/or the school network and its devices.

The Policy Review Team

The AUP was revised by the entire staff of St Colman's NS . It has been read and ratified by the Board of Management and representatives of the Parents/Teachers Association (PTA).

It is envisaged that school and parent representatives will revise the AUP annually. Before signing, the AUP should be read carefully to indicate that the conditions of use are accepted and understood. This version of the AUP was created in June 2022.

Section A - Students

The aim of the AUP 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 Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions, outlined in the AUP, will be imposed.

School Strategy

The school employs a number of strategies, taking into account the age of the pupils, in order to maximise the learning opportunities and to reduce the risks associated with accessing the internet, namely exposure to inappropriate online content and cyberbullying. The strategies are as follows:

1. Where children have access to the internet in school, it will occur under the full, uninterrupted supervision of the class teacher. Content will be subject to the restrictions of the Schools Broadband Internet Policy, which operates an automated web-filtering function of the PDST Technology in Education. The purpose of content filtering is to ensure (in so far as possible) that inappropriate websites and content are not accessible from within

schools. - See more at: http://www.pdsttechnologyineducation.ie.

Any requests for modification of the filtering provision that is in place for St Colman's NS may only be submitted by the ICT Coordinator and in consultation with the Principal.

2. The school will regularly monitor internet usage (see Children's Use of the Internet below).

3. Children will not have access to passwords or administrator accounts.

4. Uploading and downloading of non-approved software will not be permitted.

5. Virus protection software will be used and updated on a regular basis.

6. The use of students' personal pen drives, external drives, CD ROMs, and DVDs in school requires permission from the teacher.

7. 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.

8. The installation of software, whether from CD-ROM or online sources, must be preapproved and conducted by the ICT Coordinator.

9. The usage of personal CD-ROMs in the school is subject to non-violation of the software's licence agreement and adheres to points 5 and 9 above.

<u>Children's Use of the Internet</u>

1. World Wide Web

Children who have access to the internet will do so in adherence to the above strategies.

1. Before students are allowed to make use of the school's internet facility, all Parents/Guardians will be required to complete a Permission Form (Appendix 1) and return it to the Office. Permission forms will be sent home to families of new students during the September of each year and the school's database will be updated accordingly.

2. Websites that the children use in school will be previewed by their teacher before use and subject to the filters operated by the PDST and Schools Broadband programme.

3. Web Browsers are disabled on student laptops and a student-friendly browser (Kidzui) installed.

4. Teachers and students will be familiar with copyright issues relating to online learning.

5. Children will never disclose or publicise personal information.

2. Internet Chat / Social Networking / Instant Messaging (IM)

Access to internet chat rooms, social networking sites, and instant messaging services is forbidden and blocked in accordance with the Schools Broadband Internet Policy.

3. Email

1. Children's use of email is facilitated strictly in an educational context and access to personal email and/or social networking accounts is prohibited.
2. Online tasks that involve sending and receiving email (e.g. with partner schools, educational email tasks) will be teacher-led. The class teacher may 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.
3. When students are writing and sending emails from the class email account, it will be done so under the direct supervision of the teacher.
4. Children will not send or receive by any means any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person.
5. Children will not reveal their own or another person's personal details, such as home address, telephone numbers or pictures.
6. Children will never arrange a meeting with someone they only know through emails or the internet.
7. Children will note that sending and receiving email attachments is subject to the permission of their teacher.
8. Children will observe good "netiquette" (internet etiquette) at all times and will not undertake any actions that may bring the school into disrepute.

4. School Website (www.cummerns.ie)

1. The school website is evolving all the time and is updated weekly by the ICT Team.
2. Children will be given the opportunity to publish projects, artwork, and school work on the school website, with parental permission (Appendix 1).
3. The school website will not publish the names of individuals in a photograph.
4. The publication of student work will be coordinated by the teacher and/or ICT team.

5. Children will continue to own the copyright on any works published.

6. The copying of such content is prohibited without express written permission from the relevant child and his/her parent(s)/guardian(s). Upon request, permission for reproduction will only be granted when a Reproduction Permission Letter (Appendix 2) is returned to the relevant class teacher with both the child's and a parent/guardian's signatures on it.

5. Student Laptops

1. Currently, there are 33 student laptops for use within the classroom setting. Each laptop has been configured for student use. Parental Controls are enabled and student accounts are granted restricted access and control.

2. Student laptops have Microsoft Family Safety installed, which provides the ICT Team with weekly reports of student online activity on each laptop. Further, students are denied access to internet browsers such as Google Chrome and Internet Explorer etc. Rather, an age appropriate and internet-safe browser (Kidzui) has been installed as the default student browser on each laptop.

3. In the event that a web browser is accessed (or granted access), laptops are configured to block (and subsequently notify the ICT Team) any attempts by users to access content deemed to be inappropriate for our students.

6. Personal Devices

1. Currently, children are not permitted to bring their own technology in school,

2. Using a mobile phone in class, sending text messages, and the unauthorized taking of images, still or moving, is in direct breach of the Acceptable User Policy and the Mobile Phone Policy.

7. Cyberbullying

Understanding Cyber Bullying:

- Cyber bullying is the use of ICT (usually a mobile phone and/or the internet) to abuse another person.
- It can take place anywhere and can involve many people.
- Anybody can be targeted, including pupils, school staff, and members of the wider school community.

- It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, and unauthorised publication of private information or images.

There are many types of cyber-bullying. The more common types are:

1. Text messages – can be threatening or cause discomfort. Also included here is ‘Bluejacking’ (the sending of anonymous text messages over short distances using Bluetooth wireless technology)
2. Picture/video-clips via mobile phone cameras – images sent to others to make the victim feel threatened or embarrassed.
3. Mobile phone calls – silent calls, abusive messages or stealing the victim’s phone and using it to harass others, to make them believe the victim is responsible.
4. Emails – threatening or bullying emails, often sent using a pseudonym or somebody else’s name.
5. Chat room bullying – menacing or upsetting responses to children or young people when they are in a web-based chat room.
6. Instant messaging (IM) – unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger), Yahoo Chat or similar tools.
7. Bullying via websites – use of defamatory blogs (web logs), personal websites, gaming websites, and online personal ‘own web space’ sites such as You Tube, Facebook, Ask.fm, Bebo, Twitter, SnapChat, Myspace, and TikTok among others.

Procedures for preventing Cyber Bullying:

1. Staff, pupils, parents, and Board of Management (BOM) are made aware of issues surrounding cyber bullying.
2. Pupils and parents will be urged to report all incidents of cyber bullying to the school.
3. Staff CDP (Continuous Professional Development) will assist in learning about current technologies.
4. Pupils will learn about cyber bullying through Social, Personal and Health Education (SPHE), Assemblies, Friendship Week activities and other curriculum projects.
5. Pupils, parents, and staff will be involved in reviewing and revising this policy as school procedure.

6. All reports of cyber-bullying will be noted and investigated, in accordance with the school's Anti-Bullying, Mobile Phone, Child Protection, and Positive Behaviour Policies, where applicable.

7. The school will engage a speaker to facilitate a workshop on Internet Safety and mark Safer Internet Day (SID) annually.

8. Procedures in the school's Anti-Bullying and Child Protection policies shall apply.

Incidents of cyberbullying will be addressed in the context of the school's Anti-Bullying, Mobile Phone, and Positive Behaviour Policies, where applicable.

Legislation

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video recordings Act 1989
- The Data protection Act 1988

Sanctions

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. Sanctions issued will be done so in accordance with the school's Anti-Bullying Policy and Positive Behaviour Policy.

The school also reserves the right to report any illegal activities to the appropriate authorities.

Other Relevant Policies

- Child Protection Guidelines
- Positive Behaviour Policy
- Mobile Phone Policy
- Anti-Bullying Policy
- ICT Policy

Support Structures

Websites offering support and advice in the area of Internet Safety have been listed on the "Favourites" menu of each computer connected to the Internet. The following is a selection:

NCTE - http://www.ncte.ie/InternetSafety/

Webwise - http://www.webwise.ie/

Make IT Secure - http://makeitsecure.ie

Safe Internet - http://www.saferinternet.org/ww/en/pub/insafe/

Section B – Staff and Visitors

The school's computer system is provided and managed by the school and is made available to staff to further their professional development and the education of the students in the school. Access to the school's computer facilities is a privilege and not a right. Any staff member or visitor who abuses this privilege will be immediately excluded from accessing and using the computing facilities. Exclusion from using the school's computer will prevent the user from recovering files and using the facilities.

The Board of Management of St Colman's National School may change this

policy to include changes in the law or in the acceptable practice of internet use and reserves the right to make such changes without notice and whenever required. All users are responsible for ensuring that they have read and understood the current policy.

It is a requirement of St Colman's National School that all users of its network

or facilities accept and adhere to the school's Acceptable Use Policy. All staff are required to read and sign an AUP User Agreement (Appendix 3), copies of which are kept on file by the ICT Coordinator).

Compliance with this AUP is a contractual requirement. If one fails to observe the terms of

this policy, their access to facilities may be liable to termination or suspension. In the event that

access is suspended, St Colman's National School may be prepared, at its sole discretion, to restore the account on receipt of a written statement that the user will not commit any further abuse of the service. The school reserves the right to examine or delete any files that may be held on its computer network, to monitor websites visited and online activity, and to view any email messages passing through or saved on the system.

Use of Networks and the Internet

1. Users must not use the service for the transmission of illegal material. The user agrees to refrain from sending or receiving any materials which may be deemed to be offensive, abusive, indecent, hard-core or paedophile pornography, defamatory, obscene, menacing or otherwise as prohibited by current and future statutes in force. The user agrees to refrain from sending or receiving any material, which may be in breach of copyright (including intellectual property rights), confidence, privacy, or other rights.

If you are in any doubt as the legality of what you are doing, or propose to do, you should either seek independent legal advice or cease that usage.

2. Pupils' work should never be shared on social networking sites or websites other than www.swordseducatetogether.ie. Sharing or making references to a student's work, especially if it could undermine the student, is not accepted.

3. Users should be aware that the storage, distribution of, or transmission of illegal materials may lead to investigation and possible prosecution by the authorities.

4. 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 under the Computer Misuse Act.

5. 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).

6. Users must not participate in the sending of unsolicited commercial or bulk email, commonly referred to as 'spam' or 'UCE'.

7. 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.

8. Users may not divulge their computer network passwords to third parties and must take all reasonable steps to ensure that such information remains confidential. In the event of the Secretary's absence, only the Principal will have access to the office computers for administrative purposes.

9. Access to the computer network should only be made using the authorised logon name and password.

10. Activity that threatens the integrity of the school's ICT systems, or activity that attacks or corrupts other systems is forbidden. Such activity includes browsing system files and changing any system settings.

11. 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. Incidents of this nature should be reported immediately to the ICT Coordinator or member of the ICT Team. 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 virus on other devices.

12. Other users' files must never be accessed.

13. The use of the network to access and/or store inappropriate materials such as pornographic, racist, or offensive material is forbidden.

14. In the interest of protecting the network from potential virus activity, the downloading of programs, games, screensavers, and wallpapers from the internet or uploading the same from disc or CD-ROM may only be carried out by the ICT Coordinator. This does not prevent users from using images taken and/or saved by them to set their desktop backgrounds.

15. Use of the computing facilities for personal financial gain, gambling, political purposes, or advertising is forbidden.

16. Copyright of material must be respected, particularly with regard to the download and use of protected images for further use.

17. Posting anonymous messages and forwarding chain letters is forbidden.

18. The Aladdin for Schools facility within the school may not be used for inter-staff instant messaging or chat.

19. In order to protect the information that is accessible on Aladdin, users must not divulge their logon details to third parties. Any concerns or queries must be forwarded and dealt by a member of the ICT Team with Administrator rights on the Aladdin system.

20. Users of the school's file sharing system, SETNSDRIVE, may access shared resources and curriculum content both within the school (via the internal network) and remotely (from outside the school grounds). Remote access to SETNSDRIVE requires an

individual user login, the details of which must never be divulged to a third party.

21. SETNSDRIVE must only enhance the teaching and learning that takes place within the school. Files that are neither appropriate nor relevant will be deleted.

22. Only the ICT Coordinator has permission to delete files from SETNSDRIVE. Therefore, users should be fully familiar with their documents before sharing them.

23. Should a user share their own name, address, credit card or bank details etc. on the internet, it is done so at their own risk and the school accepts no responsibility.

Email

Sending and receiving email involves the same responsibilities and approach as would be used when sending or receiving any other form of communication – written or printed mail, fax, telephone call etc. Most users fully understand what would be considered appropriate and acceptable when communicating with others and should apply these considerations to their use of email. There are occasions when some users send mail or engage in online communication that others consider unacceptable - generally regarded as abusive by the online community.

If you find it difficult to determine what might be considered 'abuse' with online communication, you should realise that, in general terms, anything that might be unacceptable, and possibly illegal in other forms of communication will be equally unacceptable and possibly illegal online.

1. Users are responsible for all email sent and for contacts made that may result in email being received

2. Users must not send any emails that are likely to cause distress or any material which is offensive, indecent, obscene, menacing, or in any way unlawful.

3. Users must not use the school network, or Aladdin Schools online software to send messages or emails to any user who does not wish to receive them.

4. The school network must not be used to send or distribute unsolicited commercial mail, commonly known as 'spam', in bulk or individually.

5. Users, as senders of emails, must not use false mail headers or alter the headers of mail messages in such a way as to conceal the identity of the sender.

Wifi

St Colman’s National School is Wifi-enabled, the purpose of which is primarily to

facilitate the scope of usages present in laptops touchscreens i-pads and mobile devices such as tablets. Therefore, Wifi is configured on wireless devices that students are permitted to use. To prevent unnecessary consumption of bandwidth, enabling Wifi is limited to wireless school-use devices. Further, given that all wireless devices will connect to the school’s wireless network, they too are subject to the filtering of content that is provided under the Broadband for Schools Programme.

This policy was ratified by the Board of Management and will be reviewed periodically

Appendices

- Appendix 1: Permission Form

- Appendix 2: Reproduction Permission Letter

- Appendix 3: AUP User Agreement

Internet Acceptable Use Policy

Appendix 1: Permission Form

Dear Parent/Guardian,

Please review the school's Internet Acceptable Use Policy, (http://www.cummerns.ie) and sign and return this permission form to the Office.

School Name: St Colman's National School

Name of Student: ______________________

Class: ______________________

Parent/Guardian

As the parent or legal guardian of the above student, 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 students access unsuitable websites.

I accept the above paragraph □ I do not accept the above paragraph □

(Please tick as appropriate)

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 students' work on the school website.

I accept the above paragraph □ I do not accept the above paragraph □

(Please tick as appropriate)

Signature: ______________________________ Date: ___________________

Address: _______________________________ Telephone: ____________________

Internet Safety Acceptable Use Policy (AUP)

Appendix 3 – AUP User Agreement

As a school user of the network and internet at St Colman's N.S., I have read and

understood the Acceptable User Policy (AUP) for the use of the internet in St Colman's N.S., and by signing it, I agree to abide by the policy as stated and to accept any sanctions

which may be imposed due to misuse of the internet and non-adherence to the AUP.

I agree to follow the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained in the AUP. I agree to report any misuse of the network to the school Principal or the ICT Coordinator. If I do not follow the rules, I understand that this may result in loss of access to the internet/computer network as well as other disciplinary action.

Name: _________________

Signature: ______________

Date: __________________