



Bord Oideachais & Oiliúna
LUIMNIGH & AN CHLÁIR

LIMERICK & CLARE
Education & Training Board

FEDAMORE CNS

ACCEPTABLE USAGE POLICY AND ACCEPTANCE FORM

2024-25



Policy Area	ICT
Version	1.0
Date	Created: October 2024
Monitored	Every 3 years
Responsibility	Principal
This policy is an uncontrolled copy. Each staff member should consult school website for the latest version of this document.	

Fedamore CNS Fedamore Kilmallock Co Limerick V35KT54	Roll Number: 14067L Phone Number: 086 2061103 Email: fedamorecns@lcetb.ie Website: fedamorecns.ie
--	--

Relationship to School's Mission Statement:

Fedamore Community National School is a co-educational, multi denominational school which is underpinned by the core values of excellence in education, care, equality, community and respect. In Fedamore Community National School, we are dedicated to helping each student to achieve their individual potential. The school policies are central to ensuring the provision of quality education in a holistic manner.

This document outlines the school's policy on permitting usage of the Internet. The Policy applies to all Internet users in Fedamore Community National School (CNS) and all methods of access to and use of the Internet, electronic devices such as, but is not limited to, computer equipment, iPads, Smart TV's, PC's, Smart Phones, iPhones etc.

Fedamore CNS is committed to the use of electronic resources to enhance the

administrative, teaching and learning opportunities for students and staff. The use of electronic devices and accessing the Internet are essential and necessary skills for life, it provides information and allows people to communicate. Access to electronic devices can be highly motivating to some of our students. However, as some material on the Internet is inappropriate, students and staff are guided to utilize these resources as presented in the Acceptable Use Policy (AUP). All such usage should apply directly to the school administration or the implementation of the school curriculum.

Legislation

The school can provide information on the following legislation relating to the use of the Internet which teachers, students and parents should familiarize themselves with:

- The Data Protection Act 1988
- Video Recordings Act 1989
- Interception Act 1993
- Child Trafficking and Pornography Act 1998
- Data Protection (Amendment) Act 2003
- General Data Protection Regulation (GDPR) May 2018

1. Aims of the Policy

The aim of this Policy is to ensure:

- Students benefit from learning opportunities offered by the school's Internet/electronic resources in a safe and effective manner.
- To promote professional, ethical, lawful and productive use of the hardware and software systems and services used by the school.
- To define and prohibit unacceptable use of such systems and services.
- To educate users about their responsibilities in relation to school technology.
- To promote practices that safeguard the wellbeing of individuals in relation to technology.
- To promote practices that safeguard data related to the school and members of the school community.
- To detail the school strategy in relation to monitoring and sanctions relations to breaches of this AUP.

2. School's Strategy

The school employs several strategies to maximize learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

3.1 General Principles of AUP

- Internet sessions will always be supervised by a teacher.
- Filtering software and/or equivalent systems will be used to minimize the risk of exposure to inappropriate material.
- Technology (hardware, software, services) are provided for educational use.
- Use of school technology for personal reasons is only permitted in accordance with this policy.
- The school will regularly monitor students' internet usage.
- Training in the area of safe usage of IT and Internet Safety will be provided.
- Students will always treat others with respect and will not undertake any actions that may bring the school into disrepute.

- The school reserves the right to monitor school technology (hardware, software services) to, in collaboration with relevant authorities:
 - Prevent and/or detect crime
 - Protect its lawful interests.
 - Prevent discriminatory and harassing behaviour.

Information gathered from monitoring may be used to instigate or support disciplinary proceedings and may be disclosed to Gardaí or other relevant authorities.

In this policy 'offensive and inappropriate material / activity includes, but is not limited to:

- Pornographic or sexually explicit material.
- Discriminatory and harassing behaviour.
- Tasteless material (such as depicting injury, harassment or animal cruelty).
- Material or activity inciting hatred.
- Creating, sharing or viewing material intended to harass, offend or intimate individuals or groups.

The school may deal with incidents that take place outside the school that impact on the wellbeing of students or staff under this policy and associated policies. In such cases the school will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school and impose the appropriate sanctions. The school implements the following strategies to promote safer use of technology:

- Education on the AUP and internet safety as part of the wellbeing curriculum.
- Safer internet day activities
- CPD opportunities for teachers in the area of internet safety.
- Provide information for parents on the AUP and internet safety.
- Any incident involving technology that raises child protection issues should be reported to the schools child protection Designated Liaison Person (DLP).

3.2 General Rules

Passwords:

- The school will provide teachers/students with passwords for a number of services and devices.

You are responsible for keeping your password secure.

Things to do:

- ✓ Choose a secure password.
- ✓ The best passwords contain a mix of numbers, letters (uppercase and lowercase) and symbols.
- ✓ Most services will have their own requirements for passwords that you will follow.

Things not to do:

- ✗ You must **never** share your password with anyone.
- ✗ Do not use an insecure password - something obvious such as:
 - Your name / username or date of birth.
 - Your favourite football team / clothing brand / singer etc.
 - A password suggested by someone else.
- ✗ Do not write down your password.
- ✗ Logging in with another user's email/password will be treated as impersonating that user and will be dealt with through sanctions

Content Creation, sharing and publishing:

- The school uses a number of services and platforms for creating and sharing content. Teachers/students may be creating videos / images / presentations / websites / blogs / emails and more to be shared digitally.
- The term 'publish' below is understood to include showing support for such material ('like' or 'thumbs up') or otherwise resharing (forwarding / 'retweeting' etc).

Things to do:

- ✓ Content should be related to school activities either curricular or extracurricular.
- ✓ Content should abide by the relevant copyright laws and fair dealing. (see 'Copyright and Related Rights Act, 2000').
- ✓ Content that has been reused should be given appropriate citation / referencing.
- ✓ Content viewable by parents and the general public should be published only after it has been approved and moderated by a teacher.

Things not to do:

- ✗ Publish material that is sexually explicit or pornographic.
- ✗ Publish material that is racist or discriminatory.
- ✗ Publish material involving threatening behaviour or that promotes physical violence or harm.
- ✗ Publish material that may bring the school into disrepute.
- ✗ Publish or share material that is protected by copyright.
- ✗ Publish material related to an individual without their express knowledge and consent.
 - Including personal information, financial information, codes, passwords, usernames etc.
- ✗ Publish any personally identifiable information without consent of the teacher and your parent if you are under 18 (as per General Data Protection Regulation).
- ✗ Creating or copying 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.

Removable storage devices:

- The school provides a platform for storing and sharing files online. In the event of someone using a removable (CD / Memory Card / USB Stick).
- If the removable storage device has personal data it should be encrypted. If it has personal data related to another individual it must be encrypted (this includes photographs, videos etc).
- Teachers must never store sensitive data relating to students on removable storage.
- As per GDPR sensitive data includes: personal data revealing racial/ethnic origin, political opinions, philosophical beliefs, trade union membership, sexual orientation.

Things to do

- ✓ Get permission from a Principal/Deputy Principal before using a removable storage device in school.
- ✓ Encrypt your drive if it contains your own personal data.

Things not to do

- ✗ Store sensitive data relating to anybody on a removable storage device.
- ✗ Store offensive material as outlined above on a removable storage device.

3.3 Activity Specific Rules

World Wide Web/ School Internet

- Students will be allowed to access the Internet for educational purposes only.
- Staff will ensure students will never disclose or publicize personal information such as personal address, telephone number or email address while using the Internet.
- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Any accidental accessing or downloading of inappropriate materials must be reported immediately in accordance with school procedures.
- Usage including distributing or receiving information, school related or personal, may be monitored for unusual activity, security and or/network management reasons by the school and LCETB.
- Students are never permitted to connect to school WIFI on any device.
- The school has chosen to implement level 4 content filtering on the schools broadband network, which aligns to NCTE guidelines. This level allows access to millions of websites including games and YouTube but blocks access to blogs and social networking sites like Facebook. This content filtering applies to school devices and personal devices. For the purposes of updating our school facebook page the desktop computer in the office, the principal's laptop and the school phone are the only devices in the school that have access to Facebook.
- The school may use additional filtering technology if deemed necessary.
- Any person taking steps to bypass the content filter may be subject to disciplinary action, however, teachers may apply to have specific devices exempt from the policy for a specific task such as to build a social media presence for an extracurricular activity or student competition entry.

Things to do

- ✔ Use the school's internet connection for educational activities only.
- ✔ Report accidental accessing of inappropriate materials to the teacher /principal.

Things not to do

- ✗ Do not attempt to view or download offensive material or material covered by copyright law.
- ✗ Do not attempt to install anything on a computer without permission from a teacher/principal.

Email

- Email should only be used for educational purposes.
- Students will use approved class email accounts with permission from a teacher.
- Students will only be allowed email in the presence of the teacher or SNA.
- Students will not send or receive any material that is illegal, obscene and defamatory or that is intended to annoy or intimidate another person either in the school or to members of the school community outside of school. Such behaviour is considered as cyber-bullying and

infringes of this nature will be dealt with under our Anti-Bullying Policy.

- Students will not reveal their own or other's people's personal details, such as addresses or telephone numbers or pictures.
- Students will never arrange a face-face meeting with someone they only know through emails or Internet.
- The school reserves the right to view email from a student's account in the course of investigating a breach of the AUP.
- School email accounts will be closed when a student leaves the school. The school will provide advice on how to transfer data prior to the account closing.

Things to do

- ✓ Add a subject line to your email so the receiver will know what it is about.
- ✓ Immediately report to the Principal/Teacher the receipt of any communication that makes you feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and do not respond to any such communication.

Things not to do

- ✗ NEVER send an email from an account that is not your own.
- ✗ Do not sign up for personal services (social media, gaming sites) etc with your school email account.
- ✗ Do not download email attachments on school computers without checking with a teacher first.
- ✗ Do not give out any personal information or passwords in an email.

iPads/tablets

- Students will be given the opportunity to use iPads/tablet.
- Students will only be permitted to use apps and websites recommended by the teacher.
- When using iPads, students must follow the Internet safety rules stated above.
- iPad are shared devices. If you open an app and somebody else has left their account logged in YOU MUST log them out.
- Do not use the devices camera without permission
- Your teacher can at anytime take your iPad off you and check which apps are open and what has been saved to the camera roll
- You will lose access to the iPad if you decide to not follow any of these guidelines

Internet Chat/ Social Media

- Students are not permitted to use personal social media or instant messaging in school.
- Social media use is permitted with specific permission from, and under the supervision of a teacher for the purpose of promoting school activities (including student competitions, extracurricular activities etc).
- To resolve issues of bullying and intimidation the school may access material made public from social media accounts. The school may use this information in disciplinary procedures and work with relevant authorities where necessary.
- Activity on personal social media accounts that takes place outside of the school network may be investigated if it relates to a pattern of bullying or intimidation of pupils in the school.

Things to do

- ✓ Use social media in a safe and respectful manner.
- ✓ Report any incident of cyberbullying to the school principal or your teacher.

Things not to do

- ✗ Do not log in to or use personal social media or instant messaging accounts in the school.
- ✗ Do not record video or audio or any student or teacher for the purposes of sharing on social media.

School Website and Educational Websites

- Fedamore CNS website is currently being created. Once uploaded, students will be given the opportunity to have photographs of projects, artwork or schoolwork uploaded, in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website. Please see Photography and Videography Policy.
- The publication of student work will be coordinated by a teacher.
- Students' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.

- The school will endeavor to use digital photographs or video clips focusing on group activities. Content focusing on individual students will not be published on the school website without parental permission.
- The school website will avoid publishing the first name and last name of individuals in a photograph.
- Personal student information including home address and contact details will be omitted from school web pages.
- The school will ensure that the image files are appropriately named will not use students' names in image file names or alt tags if published on the web.
- Students will continue to own the copyright on any work published.

Personal Devices

- Student's access to personal devices are not permitted for usage in school. Students who may bring personal devices, must leave the devices in their bag throughout the day and switched off. Therefore, students can never access the Internet whilst in school on their device. Students using their own technology in school, to send nuisance text messages, or the unauthorized taking of images with a mobile phone camera, still or moving is in direct breach of the school's AUP.
- All school staff should model AUP of the school and use technology including smartphones appropriately.

Support Structures

The school will inform students and parents of key support structures and organizations should a student inadvertently access illegal material or come into contact with harmful use of the Internet. The school will hold an internet safety week each year in school to inform parents and students of the possible uses and dangers of the Internet.

Staff Responsibilities

The staff of Fedamore CNS will:

Follow the guidelines set out in this AUP.

- Monitor and supervise student use.
- Model and provide instruction in the ethical and appropriate use of technology in this school setting.
- Maintain a curricular focus.
- Ensure all parents have a signed AUP permission form before allowing student access to the internet and the network.
- Keep any usernames and passwords confidential. In accordance with GDPR all data pertaining to students and schoolwork should be password protected/ encrypted.
- Ensure computer equipment is being legally used according to the software license only.
- Ensure students do not disclose any personal information.
- Supervise student's use of and access to electronic devices and the internet.
- Never store data concerning school business on unapproved devices such as smartphones, tablets, cloud storage for example having work email on personal phones. Ensure personal/sensitive data is never taken offsite or stored on personal unapproved devices such as smartphones, USB, external storage. All school data and its back up should always be kept on the school premises.
- In the event of remote or distance learning activities staff will use the platforms agreed for communication with the school community using work email accounts, Aladdin and Seesaw or others agreed.
- Adhere to safe and ethical use of the Internet during distance learning and on keeping personal data safe when working from home.
- Sign School Policy Acceptance Form, stating that they have read, understood, agreed to and will adhere to all AUP guidelines and assume responsibility for their own actions.

Staff Use of Computer Facilities

School personnel can access the web for educational and professional purposes throughout the day. If a staff member wishes to access the web for personal purposes it should be done outside of school hours. Any student on placement from the teacher training Colleges or SNA training colleges can only have access to the computer facilities under the supervision of the class teacher. Permission should be sought from the class teacher prior to use. Computer equipment should be locked away at the end of the day. Use of the internet by staff members

to access inappropriate material whether it be pornographic, racist or offensive, is always strictly prohibited. No person will in any way alter the filtering preferences.

Sanctions

Misuse of the Internet may result in disciplinary action, in accordance with our Code of Behaviour Policy. The school also reserves the right to report any illegal activities to the appropriate authorities eg An Garda Siochana. The severity of the sanctions will depend on the nature of the infringement. Any child protection issues that arise from use of technology will be reported immediately to the child protection designated liaison person. If a student is found to have intentionally mistreated or damaged equipment the student may be refused access to the equipment in future. Where it is found that students have intentionally damaged school equipment parents will be asked to cover the cost of the damage.

Parents/Guardians

Parents/Guardians must read the AUP carefully to ensure that the conditions of use are accepted and understood. Parents/ Guardians must then sign and return the Parental/Guardian Permission Form to the school office, at the start of school academic year September 2024-June 2025 and going forward when the student is enrolled in the school.

Review and Ratification

This AUP was ratified and communicated by the Single Manager on

It is envisaged that the school will review this Policy every 3 years.

Signed:

Chairperson

Principal

Acceptable Use Policy

Parental/Guardian Permission Form

Name of Student:

Dear Parent/Guardian

As the Parent or legal Guardian of the above student, I have read Fedamore CNS 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.

(Please tick as appropriate)

I accept the above paragraph _____ I do not accept the above paragraph _____

Parent/Guardian Signature: _____ Date: _____