

# ST.FELIM'S NATIONAL SCHOOL

SN Leiter, Coill an Chollaigh, Co. Cabhain

Roll No. 18564W

Principal:

Mrs. Cathriona Molloy

LEITER

Phone/Fax: 042-9665605

BAILIEBOROUGH

Email: [office@thevalens.com](mailto:office@thevalens.com)

CO. CAVAN

Website: [www.thevalens.com](http://www.thevalens.com)



## Internet Safety: Acceptable Use Policy

### 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.

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 Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions, outlined in the AUP, will be imposed.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

- 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 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. Felim's N.S. may only be submitted after consultation with the Principal.
- The school will regularly monitor internet usage (see Children's Use of the Internet below).
- Children will not have access to administrator accounts.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of students' personal pen drives, external drives, CD ROMs, and DVDs in school requires permission from the teacher.

- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
- If a teacher wishes to integrate a web page or any other online resource 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 or similar and close the webpage prior to the lesson.

## **Children's Use of the Internet**

### **1. World Wide Web**

Pupils are permitted supervised access to the internet for educational purposes. The following guidelines must be adhered to for internet access:

- Pupils will use the internet for educational purposes only.
- Websites that the pupils use in school will be previewed by their teacher before use and subject to the filters operated by the PDST.
- Student-friendly browsers e.g. [www.kiddle.co](http://www.kiddle.co) will be used as search engines when children are using the internet.
- Teachers will select appropriate web resources for pupils when carrying out research tasks.
- Teachers and pupils will be familiar with copyright issues relating to online learning.
- Pupils will never disclose or publicise personal information.
- Pupils will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.
- Each September, teachers will teach responsible use of the internet to pupils. Pupils will sign a class charter for responsible internet use. (See Appendix 1&2 for a sample class charters)

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

- Access to internet chat rooms, social networking sites, and instant messaging services are not permitted.

### **3. Email**

- Students use of email is facilitated strictly in an educational context and access to personal email and/or social networking accounts is prohibited.
- Students may use approved class email accounts when deemed necessary. We use a variety of cloud based educational tools to support the children's learning. Students may be provided with an account to facilitate this e.g. [student@thevalens.com](mailto:student@thevalens.com). They will not have access to either receive or send emails outside thevalens.com domain, as this privilege is suspended for student accounts.
- 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.

- If students are writing and sending emails from a class email account, it will be done so under the direct supervision of the teacher.
- 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.
- Children will not reveal their own or another person's personal details, such as home address, telephone numbers or pictures.
- Children will never arrange a meeting with someone they only know through emails or the internet.
- Children will note that sending and receiving email attachments is subject to the permission of their teacher.
- 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.thevalens.com](http://www.thevalens.com))**

Our school web site is intended to:

- Provide accurate, up-to-date information about our school
- Enable pupils to publish work to a high standard, for a very wide audience including pupils, parents, staff, members of the local community and others
- Celebrate good work
- Provide pupils with the opportunity to publish their work on the internet
- Promote the school
- The publication of student work will be co-ordinated by a teacher
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will not be published on the school website without parental permission. Video clips may be password protected.

All classes may provide work for publication on the school web site. Class teachers will be responsible for ensuring that the content of the pupils' work is accurate and the quality of presentation is maintained. All material must be the author's own work, crediting other sources included and stating clearly that author's identity and/or status.

The point of contact on the web site will be the school address, telephone number and e-mail address. **We do not publish pupils' full names or photographs that identify individuals on our web pages.** Home information or individual e-mail identities will not be published. Staff will be identified by their title and surname unless they request otherwise. Permission will be sought from other individuals before they are referred to by name on any pages we publish on our website.

#### **5. Seesaw**

St. Felim's N.S uses the digital learning platform Seesaw to:

- Provide a motivating digital environment for teaching and learning.
- Enable pupils to access online resources both at home and school.

- Foster home school links between teachers, pupils and families.
- Allow children to collaborate on digital-based projects and activities, under the direct supervision of their teacher.

All classes from junior infants to 6<sup>th</sup> have access to the Seesaw platform. Permission is explicitly sought from parents/guardians each year before pupil's profiles are activated. Class teachers and the SET team are responsible for ensuring that content shared by them is accurate and suitable. All work submitted by pupils is reviewed fully before approval by the teacher.

The following protocols are followed by all staff in the correct usage of the Seesaw platform.

- During the standard school day, teachers allow children log in to the class to complete activities using the Class QR code.
- Class QR codes are displayed in a number of locations around each classroom.
- Individual home login codes are used for home learning only.

Pupils are responsible for:

- Ensuring that any content posted by them on Seesaw is appropriate and relevant.
- Only posting responses to activities that have been specifically sought by the class or SET teacher.
- Logging out of seesaw on their device at the end of each session.
- Keeping their login details secure and not sharing their details with any other pupil.

## **Safety and Protection in an Online Environment**

### **1. Personal Devices**

- Pupils are not permitted to have their own technology in school. Examples include, but are not limited to mobile phones, iPods, mp3 players, smart watches and gaming consoles. Having such items in school without prior permission is in direct breach of the school's acceptable use policy and the school's Code of Behaviour.

### **2. Cyberbullying**

#### ***Understanding Cyber Bullying:***

- Cyber bullying is the use of DT (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, TikTok, Twitter, SnapChat, Instagram and House Party, among others.

### **Procedures for preventing Cyber Bullying:**

- Staff, pupils, parents, and Board of Management (BOM) are made aware of issues surrounding cyber bullying.
- Pupils and parents will be urged to report all incidents of cyber bullying to the school.
- Staff CPD (Continuous Professional Development) will assist in learning about current technologies.
- Pupils will learn about cyber bullying through Social, Personal and Health Education (SPHE), Assemblies, Friendship Week activities and other curriculum projects.
- Pupils, parents, and staff will be involved in reviewing and revising this policy as school procedure.
- 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.
- 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 Code of Behaviour and Anti-Bullying and Mobile Phone Policies, where applicable.

### **Responsibilities of Parent/Guardians**

- Parent/Guardians must read this policy in full.
- Accept or decline to give their child permission to have access to the internet, understanding that the internet is solely used for educational purposes and that every reasonable precaution will be taken by the school to provide for online safety.
- Accept responsibility for the education of their child/children on issues of internet responsibility and safety

- Understand that having adhered to the content of this policy, the school cannot be held responsible if their child/children tries to access unsuitable material
- Accept or decline to give the school permission to put their child's work and/or accomplishment together with the child's name and/or photograph on the school website

### **Consent**

As part of this policy parents must give permission for their child to access the internet and to allow their child's work be uploaded on the school website if necessary. These permissions are sought on our school's registration form, that is completed by parents when they accept a place offered to their child in our school. These permissions are also updated annually via a Microsoft Form or the Aladdin Connect App.

### **Legislation**

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video recordings Act 1989
- The Data Protection Act 1988
- Data Protection Act 2018

### **Sanctions**

The normal school rules will apply. Misuse of the internet may result in disciplinary action, including verbal and written warnings, withdrawal of access privileges, consequence sheets and, in extreme cases, suspension or expulsion. Sanctions issued will be done so in accordance with the school's Code of Behaviour and Anti-Bullying Policy. The school also reserves the right to report any illegal activities to the appropriate authorities.

### **Other Relevant Policies**

- Child Safeguarding Statement
- Code of Behaviour
- Remote Teaching and Learning Policy
- Mobile Phone Guidelines
- Anti-Bullying Policy
- ICT Policy

### **Support Structures**

The following websites are a selection of websites that offer support and advice in the area of Internet Safety:

- NCTE - <http://www.ncte.ie/InternetSafety/>
- Webwise - <http://www.webwise.ie/>
- Make IT Secure - <http://makeitsecure>.
- 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.

It is a requirement of St. Felim's National School that all users of its network or facilities accept and adhere to the school's Acceptable Use Policy.

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.

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.

In the event that access is suspended, St. Felim'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 Board of Management of St. Felim'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.

### **Use of Devices, Networks and the Internet**

- 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.*

- Pupils' work should never be shared on social networking sites or websites other than [www.thevalens.com](http://www.thevalens.com) or Seesaw. Sharing or making references to a student's work, especially if it could undermine the student, is not accepted.
- 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.

- 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.
- 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 Principal. Additionally, anti-virus software is used to prevent virus activity, the school accepts no responsibility for damage caused by computer virus on other devices.
- The use of the network to access and/or store inappropriate materials such as pornographic, racist, or offensive material is forbidden.
- Use of the computing facilities for personal financial gain, gambling, political purposes, or advertising is forbidden.
- Copyright of material must be respected, particularly with regard to the download and use of protected images for further use.
- The *Aladdin for Schools* facility within the school may not be used for inter-staff instant messaging or chat.
- In order to protect the information that is accessible on Aladdin, users must not divulge their login details to third parties.
- Users of the school's cloud based file sharing system, One-Drive, may access shared resources and curriculum content
- 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.

### **Guidelines for staff for the use of School Devices**

#### **General Guidelines**

1. School devices e.g. a laptop/iPad remain the property of St. Felim's N.S. at all times.
2. School devices are provided to teachers employed by St. Felim's N.S. for the purpose of assisting them in their duties as teachers of the pupils in St. Felim's N.S. in line with all relevant school policies. If a teacher's employment in St. Felim's N.S. ceases, school devices must be returned.
3. School devices may be used for incidental personal use as long as such use does not interfere with the teacher's job, duties and performance with system operations or other system users. 'Incidental personal use' is defined as use by an individual employee for occasional personal communications. Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules, and must take place outside of official school opening times.
4. School devices are covered under school insurance, however, the teacher must take reasonable care to avoid damage or loss. All leads and accessories are to be stored safely.



5. If a school device is damaged, lost or stolen, the incident must be reported to the Principal as soon as possible

## **Guidelines for Use**

1. School devices must be password protected. The use of screensavers is strongly advised.
2. School devices must not be left unattended or unsecured in a classroom, or other place in the school, at home or in a public place.
3. School devices must not be left in plain view in an unattended or unsecured vehicle.
4. School devices are not to be accessed by any other person unless authorised by St. Felim's N.S.
5. School devices must not be interfered with, tampered with or altered by a third party or otherwise except in accordance with clause.
6. School devices will be used to access pupil information both at home and at school and as such, the school's data protection policy must be complied with when accessing and processing such data.
7. Pupils cannot use a teacher's device unsupervised unless guided access is enabled.

## **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. In general terms, anything that might be unacceptable, and possibly illegal in other forms of communication will be equally unacceptable and possibly illegal online.

- Users are responsible for all email sent and for contacts made that may result in email being received.
- 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.
- 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.
- The school network must not be used to send or distribute unsolicited commercial mail, commonly known as 'spam', in bulk or individually.
- 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.
- Email functionality is disabled for student accounts.

## **Wifi**

St. Felim's National School is Wifi-enabled, the purpose of which is primarily to facilitate the scope of usages present in laptops and other mobile devices such as tablets. Therefore, Wifi

is configured on wireless devices that students are permitted to use. 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.

## **Implementation and Review**

### **1. Roles and Responsibilities**

It will be the responsibility of the staff and pupils to implement the policy. Parents and the Board of management will support the plan.

### **2. Time Frame and Review**

It will be reviewed as often as required when changes occur but will be reviewed by the whole school in the school year 2023/2024.

### **Ratification**

This policy was ratified by the Board of Management at its meeting on \_\_\_\_\_.

Signed: \_\_\_\_\_  
Gerry Sheanon (Chairperson B.O.M.)

Signed: \_\_\_\_\_  
Cathriona Molloy (Principal.)

# ST.FELIM'S NATIONAL SCHOOL

SN Leiter, Coill an Chollaigh, Co. Cabhain

Roll No. 18564W

Principal:

Mrs. Cathriona Molloy

LEITER

Phone/Fax: 042-9665605

BAILIEBOROUGH

Email: [office@thevalens.com](mailto:office@thevalens.com)

CO. CAVAN

Website: [www.thevalens.com](http://www.thevalens.com)



## **Appendix 1 – Sample Class Charter for Responsible Internet Use (Junior Classes)**

**We use school iPads/laptops and internet connection for learning.**

**These rules will help us to be fair to others and keep everyone safe.**

- I will only use an iPad/laptop when directed by my teacher or adult
- I will only use activities that a teacher or an adult has told or allowed me to use.
- I will take care of the iPad/laptop and other equipment.
- I will ask for help from a teacher or an adult if I am not sure what to do or if I think I have done something wrong.
- I will turn the screen off and tell a teacher or an adult if I see something that upsets me.
- I know that if I break the rules I might not be allowed to use a school iPad/laptop.

# ST.FELIM'S NATIONAL SCHOOL

SN Leiter, Coill an Chollaigh, Co. Cabhain

Roll No. 18564W

Principal:

Mrs. Cathriona Molloy

LEITER

Phone/Fax: 042-9665605

BAILIEBOROUGH

Email: [office@thevalens.com](mailto:office@thevalens.com)

CO. CAVAN

Website: [www.thevalens.com](http://www.thevalens.com)



## **Appendix 2 – Sample Class Charter for Responsible Internet Use (Senior Classes)**

**We use school iPads/laptops and internet connection for learning.**

**These rules will help us to be fair to others and keep everyone safe.**

- I will only use an iPad/laptop when directed by my teacher or adult
- I will use child friendly search engines when using the computers to search for websites, unless my teacher has already approved that site.
- I will take care of the iPad/laptop and other equipment.
- I will ask for help from a teacher or an adult if I am not sure what to do or if I think I have done something wrong.
- When logging into the iPad/laptop, I will use my own login and password, which I will keep secret.
- I will only use activities that a teacher or an adult has told or allowed me to use. I will not use internet chat.
- When communicating online, I will not give out my home address, phone number, or arrange to meet anyone. I will only chat to people I know, or my teacher has approved and my messages will be polite and sensible.
- If I see anything that I am unhappy with or I receive messages I do not like, I will turn off the screen and tell a teacher immediately.
- I know that the school will check my work and online storage space and may monitor the internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the internet or school iPad/laptop.