

Scoil Bhríde, Ráth Chormaic

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.

The Policy Review Team

The AUP was revised by the ICT Policy Review Team in the school: Noelle Crowley and Margaret Howard. These individuals also constitute part of the Digital Learning Team in Scoil Bhríde as of the below date (it is expected that other staff/Board members will join the Digital Learning Team going forward).

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 May 2020 and reviewed in September 2024.

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 Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions, outlined in the AUP, will be imposed.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 or Special Education 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 Scoil Bhríde may only be submitted by the ICT Coordinator and in consultation with the Principal.
2. Children will not have access to administrator accounts.
3. Uploading and downloading of non-approved software will not be permitted.
4. Virus protection software will be used and updated on a regular basis.
5. The use of students' personal USB drives, external drives, CD ROMs, and DVDs in school requires permission from the teacher.
6. 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.
7. The installation of software, whether from CD-ROM or online sources, must be preapproved by the ICT Coordinator.
8. The usage of personal CD-ROMs in the school is subject to non-violation of the software's license

agreement and adheres to points 5 and 7 above.

9. Scoil Bhríde takes every reasonable precaution to provide for online safety but cannot be held responsible if students access unsuitable websites either deliberately or inadvertently.

Children's Use of the Internet

Internet (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). From May 2020 this permission form will be consented to by parents through Aladdin Connect each year and 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. Teachers and students will be familiar with copyright issues relating to online learning.
4. Children will never disclose or publicise personal information.

Internet Chat / Social Networking / Instant Messaging (IM)

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

Email/Google Drive

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. Teachers may set up email addresses and log-in details for students through GSuite for the purpose of accessing and using educational sites where individual logins are required by students.
3. When using Google Classroom and the GSuite Apps, students will use approved class email accounts under supervision of a teacher or parent/guardian.
4. Teachers may set up log-in details for students to access educational programmes such as spelling programmes.
5. 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.
6. When students are writing and sending emails from the class email account, it will be done so under the **direct supervision of the teacher**.
7. 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.
8. Children will not reveal their own or another person's personal details, such as home address, telephone numbers or pictures.
9. Children will never arrange a meeting with someone they only know through emails or the internet.
10. Children will note that sending and receiving email attachments is subject to the permission of their teacher.
11. Children will observe good "netiquette" (internet etiquette) at all times and will not undertake any actions that may bring the school into disrepute.

Distance Learning

1. In circumstances where teaching cannot be conducted on the school premises, teachers may use Google Classroom, Google Meet, Zoom, SeeSaw, Padlet, Typing.com, MangaHigh, Read Theory or other platforms approved by the Principal as platforms to assist with remote teaching where necessary.
2. In the case of Google Classroom and Google Meet, parents/guardians must grant access to their child to have a school Gmail address such as initialandsurnameyearofgraduation@sbrathcormac.ie 3. Parents/guardians will be provided with the Gmail password and will be expected to monitor their child's use of the Gmail address and Online Platforms.
4. If teachers are using Zoom, parents/guardians must consent to their child having a school email address as above to allow their child access to the lessons. Where the child does not have a school email address, parents can consent by submitting their own email address for their child to access lessons on Zoom.
5. Parents/guardians must also agree to monitor their child's participation in any such lessons conducted on the Online Platforms.

School Website (www.sbrathcormac.ie)

1. The school website is evolving all the time and is updated regularly by class teachers, school secretary and school principal.
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 Digital Learning 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.

Student Laptops, iPads and Chromebooks

1. Currently, there are 27 iPads and 30 Chromebooks for use within the classroom setting. These are configured for student use and student accounts (where applicable) are granted restricted access and control.

Personal Devices

1. Children using their own technology in school, such as tablet devices, may do so **only** with the written approval of the Board of Management, as part of a specific and structured learning programme designed by the school.
2. The school strongly advises against the possession of a mobile phone. The use of a mobile phone during school hours, on school grounds and during school activities, which includes matches and tours, is in direct breach of the Acceptable Use Policy and the Mobile Phone Rule. The school takes no responsibility for the loss, damage or theft of mobile phones.
3. The possession and use of smart watches or devices with the capacity to take images, still or moving, is in direct breach of the Acceptable Use Policy.

Photographs and Videos

Occasionally, we may take photographs of the children in our school. Our school likes to celebrate your child's work and achievements. As a result, images of your child and their work may appear in school displays and on our school website.

Videos of children's involvement in group activities may also be taken for the school website. Children's names will not be included with the photos or videos on the school website. On occasions such as school shows, sports days, matches, Communion, Confirmation and other school events, local press photographers take photographs. These images may appear in local publications such as: Avondhu, Cork Man, Evening Echo, Irish Examiner, Imokilly News.

Use of Assistive Technology

There is a wide range of technological or software support available which can provide assistance to pupils in schools and which has potential to assist children in their academic performance, learning, completion of homework, or which could assist them to achieve a degree of improvement to their educational performance. All children have particular educational needs and accordingly, it is acknowledged that all children could potentially benefit from, or achieve a degree of improvement to their performance in school, through the provision of technological support or equipment, such as personal computers. The equipment provided for under the Assistive Technology Scheme, however, is specialist equipment of a nature beyond that which can normally be provided to pupils by schools through general funding. Provision under this scheme is made for those pupils whose degree of physical and/or communicative disability is such that without technological support it will not be possible for them to access the school curriculum. (Circular 0010/2013). Children who have been granted access to this scheme may use this specialist equipment with the consent of parents/guardians. The User Agreement (Appendix 4) must be signed first.

Cyberbullying

Understanding Cyber Bullying:

- Cyber bullying is the use of ICT (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 Whatsapp, Yahoo Chat, Viber, Facebook Messenger 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 YouTube, Facebook, Ask.fm, Instagram, Twitter, SnapChat, and Myspace, 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 CPD (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,

programmes such as HTML Heroes and My Selfie: My World, anti-bullying lessons and other curricular 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 (Rules), Child Protection and Behaviour Policies etc., where applicable. 7. The school will engage a speaker Community Guard to facilitate a workshop on Internet Safety for 5th – 6th Classes 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, Child Protection and Behaviour Policies, as appropriate.

Legislation

- E.U. General Data Protection Regulations 2018
- Anti-Bullying Guidelines for Primary Schools 2013
- 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 Behaviour Policy. The school also reserves the right to report any illegal activities to the appropriate authorities.

Other Relevant Policies

- Child Protection Policy/Guidelines
- Child Safeguarding Statement
- Code of Behaviour Policy
- Anti-Bullying Policy
- Data Protection Policy
- Teachers Code of Conduct
- Complaints and Grievance Procedures

Support Structures

Websites offering support and advice in the area of Internet Safety are listed below. This list is not exhaustive and will be made available to teachers in the 'Resources' section of the Scoil Bhríde Drive.

- 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/>

Other websites include:

www.spunout.ie

www.childnet.int.org

www.antibullying.net

www.kidsmart.org.uk/beingsmart

www.bbc.co.uk/schools/bullying
www.childline.ie/index.php/support/bullying/1395
www.chatdanger.com
www.kidpower.org
www.sticksandstones.ie
www.abc.tcd.ie

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 Scoil Bhríde 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 the Board of Management of Scoil Bhríde 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, management of Scoil Bhríde 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.

Sanctions

If there is a breach of the AUP by a user, the Board of Management has the right to refer to the necessary policies such as Teachers Professional Code of Conduct (Teaching Council), Grievance and Complaints Procedure (INTO/CPSMA) etc., and carry out appropriate sanctions if required.

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, pornographic, 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.
2. Pupils' work should never be shared on social networking sites or websites other than www.sbrathcormac.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 and Deputy Principal will have access to the office computer for administrative purposes.
9. Access to the computer network and/or Aladdin for Schools system should only be made using the authorised login 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 Digital Learning Team. Additionally, while anti-virus software is used to prevent virus activity, the school accepts no responsibility for damage caused by a 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 login details to third parties. Any concerns or queries must be forwarded and dealt with by a member of the ICT Team with Administrator rights on the Aladdin system.
20. Users of the school's file sharing system, Google Drive, may access shared resources and curriculum content both within the school and from outside the school grounds.
21. 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

Internet Safety: Acceptable Use Policy (AUP)

Appendix 1: Permission Form

(Consent for the following questions will be received via Aladdin)

Parental Consent

		Yes	No
1.	I give permission for my child's photograph to be used within the school for display purposes.		
2.	I give permission for my child's photograph to be used on the school website.		
3.	I give permission for a video of my child's involvement in a group activity to be used on the school website.		
4.	I understand and accept the terms of the Acceptable Use Policy relating to publishing students' work on the school website and I give permission for my child's work to be published on the school website.		
5.	I give permission for my child's photograph to appear in local publications such as: Avondhu, Cork Man, Evening Echo, Irish Examiner, Imokilly News.		
6.	I give permission for my child to have a school @sbrathcormac.ie address for the purpose of educational programme log-ins.		
7.	I give permission for my child to use online platforms such as: Google Classroom, Padlet, Seesaw, Typing.com, MangaHigh, Read Theory and ClassDojo.		
8.	I give permission for my child to participate in teacher-led video platforms such as Google Meet and Zoom.		
9.	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.		

Parent's Signature: _____ Date: _____

Internet Safety: Acceptable Use Policy (AUP)

Appendix 2: Reproduction Permission Letter

I _____ (Child's name) and _____ (Parent/Guardian's name) give permission to
_____ (Person(s) requesting permission) to reproduce work belonging to
_____ from the school website (www.sbrathcormac.ie).

Parent/Guardian Date

Internet Safety: Acceptable Use Policy (AUP)

Appendix 3: AUP User Agreement for Staff

As a school user of the network and internet at Scoil Bhríde, I have read and understood the Acceptable User Policy (AUP) for the use of the internet in Scoil Bhríde, 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: _____ (print)

Signature: _____

Date: _____

Internet Safety: Acceptable Use Policy (AUP)

Appendix 4: Agreement for Children using Digital Technology

under the Assistive Technology

Terms and Conditions:

1. The laptop (or any other approved assistive technology/equipment) remains the property of Scoil Bhríde, Rathcormac (the 'School').
2. Should the designated pupil change school, including to post primary, the School will consult with the SENO with regard to the transfer of any approved assistive technology/equipment with the pupil where it is still appropriate for the pupil's assessed needs. The final decision regarding transfer will rest with the School Board of Management.
3. The laptop (or any other approved assistive technology/equipment) will be used solely by the designated pupil and will not be used by or transferred to a third party.
4. The parent will remind and teach their child to take due care of the laptop (or any other approved assistive technology/equipment) at all times when handling, transporting and using the laptop/equipment.
 - It is not to be left unattended in a public place.
 - It is not to be left unattended in a classroom or other place in the school.
 - All laptop/device leads must be unplugged from sockets and all accessories are to be stored safely and securely in the case, with the device when work is complete.
 - It is not to be left in plain view in an unattended or unsecured vehicle but kept out of sight in the locked boot. - It is not to be interfered with, tampered with or altered by a third party.
 - It is not to be used in the vicinity of food, drinks or chemicals.
5. The laptop/device will be used solely to assist with typing skills, completion of homework assignments and other school related activities. Only school approved software packages/applications may be used.
6. The designated pupil will have use of the device each evening from Monday to Thursday during school terms and it is to be returned to the school on Fridays for safe keeping over the weekends.
7. The laptop must be returned to the school in good working order on or before the last day of the school year or earlier if requested by the School.
8. The laptop is covered under school insurance, however, the parent must take reasonable care to avoid damage or loss.

School insurance provides protection from standard risk but excludes theft from a vehicle when laptop is left visible.

9. Use of the laptop and including all internet usage will be supervised by a parent and will be of an appropriate nature to minimise pupil's exposure to inappropriate material.

10. The School will make regular checks to update the laptop/device, ensuring that anti-virus software is kept up to date and also to check for inappropriate use.

11. The laptop or device will be used lawfully and in accordance with the school's Acceptable Use Policy regarding the ethical use of technology, use of legal software, use of the Internet and the protection of personal data. The parent shall agree to review and adhere to the current School Acceptable Use Policy, specifically where this policy relates to the safe and appropriate use of approved IT equipment such as laptops.

12. The following is deemed by the School as being completely unacceptable and will result in the equipment being reclaimed:

-Accessing, transmitting or receiving obscene or pornographic material.

- Engaging in cyber cheating or plagiarism (taking material created by others and presenting it as if it were one's own) -

Engaging in cyber bullying

-Downloading or loading software or applications that are not approved by the school

13. The laptop/device will be kept in good working order. All faults, defects or malfunctions while in the care of the pupil are to be reported to the Principal or Class Teacher who will inform the teacher with responsibility for the servicing and upkeep of the laptop.

14. Any repairs necessary due to damage caused to the laptop/device while in the care of the pupil will be arranged by the school and paid for by the parent of the pupil.

15. The laptop/device will not be sold, assigned, transferred or otherwise disposed of.

16. Laptop/Device markings, tags or plates or engravings will not be removed, concealed or altered. The laptop must not be marked in any way that might reduce the value of the laptop.

17. If the laptop or device is lost, stolen or damaged the parent will advise the Principal and the Gardaí as soon as possible orally and in writing including all relevant details, record of events etc.

18. Due to current software licensing arrangements covering home use, the laptop or device package cannot be used for any commercial purpose.

19. If any of these terms or conditions are breached, the School Board of Management may at any time revoke this arrangement.

Please note: The School's Acceptable Use Policy can be viewed on www.sbrathcormac.ie

Agreement for Signing by Pupil and Parent under the Assistive Technology Scheme

Re: The Home Use of School Owned Assistive Technology

Laptop Make/Brand	
Laptop Serial Number	
Value of Laptop	
List of Software installed	
Value of Software installed	
List accompanying equipment (e.g. microphone, headphones etc.) please describe each item (brand etc.)	
Value of accompanying equipment (please list in full)	
<i>I confirm that I accept responsibility for taking into my possession a laptop which is the property of Scoil Bhríde, Rathcormac, County Cork. Roll Number: 17609N after school on weeknights when my child requires it. I confirm that I have read, fully understand and accept the Terms and Conditions attached to this policy and agreement and other relevant policies as are determined by Scoil Bhríde, Rathcormac, County Cork.</i>	
Name of Pupil (Block Capitals)	
Pupil's Class when this agreement was signed	
Pupil's Teacher when this agreement was signed	

Signature of Pupil	
Name of Parent/Guardian (Block Capitals)	
Signature of Parent/Guardian	
Date	

Address of Parent/Guardian		
Contact Numbers	Mobile:	Home:
Signature of Principal		