Coláiste Cholmcille

School Roll No. 91506V

Internet Acceptable Use Policy

2015

Coláiste Cholmcille, Ballyshannon, is a community which respects the rights and self-worth of all, and aims to provide a happy and safe environment in which the individual may achieve her/his spiritual, academic and personal potential.

— CCBS Mission Statement

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. They are as follows: John Kennedy (ICT Coordinator), Damian Conlon, Conor Beattie, Hugh Mc Glynn, and Emma McKinley. 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 on a three year basis.

Parents: It is understood that by enrolling your daughter/son in our school that you as a parent and your son/daughter read carefully this AUP and in doing so are aware of the contents and conditions of use and that these are accepted and understood and furthermore agree to adhere to the obligations set out herein.

School Management: The Board of Management of Coláiste Cholmcille is a statutory Board appointed pursuant to the provisions of the Education Act 1998.

Original Version created September 2004, and ratified by **Board of Management, Staff, Parents and Students of Coláiste Cholmcille, Ballyshannon.**

Latest revision September 2014.

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 Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions, outlined in the AUP, will be imposed.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 students have access to the internet in school, it will occur under the 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 Coláiste Cholmcille may only be submitted by the ICT Coordinator and in consultation with the Principal.
- The school will regularly monitor internet usage (see Students Use of the Internet below).
- Students **will not** have access to Staff passwords or 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.
- 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 suitable format and use this in the lesson.
- The installation of software, whether from CD-ROM or online sources, must be previewed and deemed appropriate.
- 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 6 above.

World Wide Web

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

- By enrolling in the school it is understood that students are allowed to make use of the school's internet facility, with Parents/Guardians permission. Parents who do not want their daughter/son to access these facilities ***must inform the school in writing***, during the **September** of each year and the school's database will be updated accordingly.
- Websites that the students use in school will be previewed by their teacher before use and subject to the filters operated by the PDST and Schools Broadband programme.
- Teachers and students will be familiar with copyright issues relating to online learning.
- Students will never disclose or publicise personal information.

Internet Chat / Social Networking / Instant Messaging (IM)

- Students will only have access to chat rooms, discussion forums or other electronic communication forums that have been approved by the school.
- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.
- Face-to-face meetings with someone organised via Internet chat will be forbidden.

Email

- Students use of email is encouraged but is strictly in an educational context and access to personal email and/or social networking accounts is prohibited.
- Online tasks that involve sending and receiving email (e.g. with partner schools, educational email tasks) will be teacher-led. All emails will be reviewed by the teacher prior to sending if deemed necessary.
- When students are writing and sending emails for school purposes, it will be done so under the direct supervision of the teacher.
- Students 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.
- Students will not reveal their own or another person's personal details, such as home address, telephone numbers or pictures.
- Students will never arrange a meeting with someone they only know through emails or the internet.
- Students will note that sending and receiving email attachments is subject to the permission of their teacher.

- Students 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.ccbs.ie)**

- The school website is evolving all the time and is updated weekly by **Mr. Conor Beattie.**
- Students are given the opportunity to publish projects, artwork, and school work on the school website.
- The school website will only publish the names of individuals in a photograph with the individual's permission.
- The publication of student work will be coordinated by their teacher and/or Mr. Conor Beattie.
- Students will continue to own the copyright on any works published.
- 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**

- Currently, there are a number of student laptops for use within the classroom setting. Each laptop has been configured for student use. The use of these laptops within school fall under the same conditions as all other PC's within the control of the school Network.

6. **Personal Devices**

- Currently, students using their own technology in school, such as tablet devices, do so with the approval of the Board of Management, as part of a specific and structured learning programme designed by the school.
- Using a mobile phone in class is permitted with teacher approval and for educational purposes only, otherwise 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:

- 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)
- Picture/video-clips via mobile phone cameras – images sent to others to make the victim feel threatened or embarrassed.
- 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.
- Emails – threatening or bullying emails, often sent using a pseudonym or somebody else's name.
- Chat room bullying – menacing or upsetting responses to children or young people when they are in a web-based chat room.
- Instant messaging (IM) – unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger), Yahoo Chat or similar tools.
- 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, WhatsApp, Twitter and SnapChat, 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 CDP (Continuous Professional Development) will assist in learning about current technologies.

- Pupils will learn about cyber bullying through Social, Personal and Health Education (SPHE), Assemblies, Student Mentoring 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.
- The school will engage in a heightened awareness week annually on Internet Safety and mark Safer Internet Day (SID) with the entire student cohort.
- 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/
- MakeITSecure- http://www.makeitsecure.ie
- Safe Internet - http://www.saferinternet.org/ww/en/pub/insafe/

www.spunout.ie	www.childnet.int.org
www.childline.ie/index.php/support/bullying/1395	www.antibullying.net
www.chatdanger.com	www.kidpower.org
www.bbc.co.uk/schools/bullying	www.kidsmart.org.uk/beingsmart
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 Coláiste Cholmcille 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 Coláiste Cholmcille 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 2), copies of which will be 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, Coláiste Cholmcille 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

- 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.ccbs.ie. Sharing or making references to a student's work, especially if it could undermine the student, is not accepted.
- Users should be aware that the storage, distribution of, or transmission of illegal materials may lead to investigation and possible prosecution by the authorities.
- 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.
- 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).
- Users must not participate in the sending of unsolicited commercial or bulk email, commonly referred to as 'spam' or 'UCE'.
- 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.
- 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.
- Access to the computer network should only be made using the authorised logon name and password.
- 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 ICT Coordinator or Network Administrator. 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.

- Other users' files must never be accessed.
- The use of the network to access and/or store inappropriate materials such as pornographic, racist, or offensive material is forbidden.
- 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.
- 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.
- Posting anonymous messages and forwarding chain letters is forbidden.
- In order to protect the information that is accessible on the network and members 'U'DRIVE, users must not divulge their logon details to third parties. Any concerns or queries must be forwarded to and dealt with, by the ICT Coordinator or Network Administrator
- Users of the school's file sharing system, 'U'DRIVE, may access shared resources and curriculum content within the school (via the internal network).
- External access to school files may be coordinated through Office 365 and the relevant staff OneDrive. Training is provided in this to all Staff members.
- 'U'DRIVEs must only be used to enhance the teaching and learning that takes place within the school. Files that are neither appropriate nor relevant will be deleted.
- Only the ICT Coordinator has permission to delete files from 'U'DRIVEs. Therefore, users should be fully familiar with their documents before sharing them.
- 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.

- 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, 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.

Wifi

Coláiste Cholmcille is Wi-Fi-enabled, the purpose of which is primarily to facilitate the scope of usages present in laptops and other mobile devices such as tablets phones etc. 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. All staff members will have access to the CCBS network and passwords are provided on request. Under no circumstances are schools passwords for Wifi provided to staff be shared with students.

Ratified by Board of Management

_____ _____

Chairperson, Board of Management Date

Appendices

- Appendix 1: Reproduction Permission Letter

- Appendix 2: AUP User Agreement

Internet Safety Acceptable Use Policy

Appendix 1:

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.ccbs.ie).

_____ Parent/Guardian

_____ Date

Internet Safety Acceptable Use Policy (AUP)

Appendix 2:

AUP User Agreement

As a school user of the network and internet at Coláiste Cholmcille Community School, I have read and understood the Acceptable User Policy (AUP) for the use of the internet in Coláiste Cholmcille 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: _____