Student Acceptable Use Policy

1.0 Introduction

Colaiste Choilm CBS recognizes that access to Information and Communication Technology (ICT) gives our students enhanced opportunities to learn, engage, communicate and develop skills that will prepare them for many aspects of life.
To that end, **Colaiste Choilm CBS** provides access to ICT for student use.
This ***Acceptable Use Policy*** outlines the guidelines and behaviours that our students are expected to follow when using school technologies or when using personally-owned devices on the **Colaiste Choilm CBS** campus or at **Colaiste Choilm CBS** organised activities.

1.1 Technologies Covered

Colaiste Choilm CBS may provide students with Internet access, desktop computers, digital imaging equipment, laptop or tablet devices, video-conferencing capabilities, virtual learning environments, online collaboration capabilities, online discussion forums, email and more.
As new technologies emerge, **Colaiste Choilm CBS** may provide access to them also.
The policies outlined in this document are intended to cover all online technologies used in the school, not just those specifically mentioned.

1.2 Colaiste Choilm CBS ICT Network

Colaiste Choilm CBS computer network is intended for educational purposes

- All activity over the network may be monitored and retained
- Access to online content via the network is restricted in accordance with our policies and *the Department of Education and Skills* through its agency, the *National Centre for Technology in Education*

Students are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a student believes it shouldn't be, the student can ask his/her teacher submit the site for review. This is done via the *National Centre for Technology in Education's* filtering service *FortiGuard*

- Students are expected to follow the same rules for good behaviour and respectful conduct online as offline – these rules are found in the **Colaiste Choilm CBS's** existing *Code of Behaviour*
- Misuse of school resources may result in disciplinary action
- We make a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from misuse of school technologies
- Students are expected to alert his/her teacher immediately of any concerns for safety or security

1.3 Colaiste Choilm CBS email and online collaboration

Colaiste Choilm CBS may provide students with email accounts for the purpose of school-related communication. Availability and use is restricted based on school policies.
Email accounts should be used with care. Email usage may be monitored and archived.
Colaiste Choilm CBS recognises that online collaboration is essential to education and may provide students with access to a variety of online tools that allow communication, sharing, and messaging among students.
Students are expected to communicate with the same appropriate, safe, mindful and courteous conduct online as offline.

1.4 Colaiste Choilm CBS's own mobile devices

Colaiste Choilm CBS may provide students with mobile computers, digital recorders or other devices to promote learning both inside and outside of the school. Students should abide by the same expected use policies, when using school devices off the school network, as on the school network.
Students are expected to treat these devices with respect. They should report any loss, damage, or malfunction to their teacher staff immediately. Students may be financially accountable for any damage resulting from negligence or misuse. Use of school-issued mobile devices will be monitored.

1.5 Mobile devices in the possession of Colaiste Choilm CBS students

Students may NOT use personally-owned devices (e.g. laptops, tablets-computers, digital-cameras, and smart-phones) while on the school premises

1.6 Colaiste Choilm CBS Security

Students are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programmes and not opening files or programmes of unknown or un-trusted origin.

Use commom sense if you think a website does not look right. Inform your teacher. Think twice before you click on anything you feel is not right.

If you believe a computer or mobile device you are using might be infected with a virus, please alert your teacher.

Do not attempt to remove the virus yourself or download any programmes to help remove the virus.

Students should not download or attempt to download or run *.exe* programmes over the school network or onto school resources. You may be able to download other file types, such as images of videos.

For the security of our network, download such files only from reputable sites, and only for educational purposes.

1.7 Netiquette

Netiquette may be defined as appropriate social behaviour over computer networks and in particular in the online environment. To this end

- Students should always use the Internet, network resources, and online sites in a courteous and respectful manner
- Students should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Students should use trusted sources when conducting research via the Internet
- Students should not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it is out there - and can sometimes be shared and spread in ways you never intended

More detailed examples of expected use and unacceptable use are given in Appendices One and Two.

1.8 Personal Safety

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the immediate attention of

- a teacher if you are at school
- a parent / guardian if you are at home
- Students should never share personal information about themselves or others, including phone numbers, addresses, PPS numbers and birth-dates over the Internet without adult permission
- Students should never agree to meet someone they meet online in real life without parental permission.

1.9 Cyber-bullying

Harassing, flaming, denigrating, impersonating, outing, tricking, excluding and cyber-stalking are all examples of cyber-bullying.

- Such bullying will not be tolerated in **Colaiste Choilm CBS**
- Don't be mean. Don't send emails or post comments or photos with the intent of scaring, hurting, or intimidating someone else
- Engaging in any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges
- In some cases, cyber-bullying is a crime
- Remember that your activities are monitored and retained
- The school will support students, teachers and parents in dealing with cyber-bullying. Colaiste Choilm CBS is committed to the *Child Protection Procedures for Primary and Post-Primary Schools (Circular 0065/2011)* and will act as required by the *Department of Education and Skills*, the *Department of Children and Youth Affairs*, *the Department of Justice and Equality* and the *Health Service Executive*.

1.10 Violations of this Acceptable Use Policy

Violations of this policy in Colaiste Choilm CBS may have disciplinary repercussions, including:

- Suspension of network and computer privileges
- Notification to parents in most cases
- Detention
- Suspension from school and/or school-related activities
- Expulsion
- Legal action and/or prosecution

I have read and understood this Acceptable Use Policy and agree to abide by it:

_____(Student Signature)

I have read and discussed this Acceptable Use Policy with my child:

_____(Parent / Guardian Signature)

Appendix 1 Examples of Acceptable Use

I will:

- Use school technologies for school-related activities and research.
- Follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline.
- Treat school resources carefully, and alert teachers if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits only.
- Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
- Recognise that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of school resources.

This is not intended to be an exhaustive list. Students should use their own good judgment when using school technologies.

Appendix 2 Examples of Unacceptable Use

I will not:

- Use school technologies in a way that could be personally or physically harmful to myself or others.
- Search inappropriate images or content.
- Engage in cyber-bullying, harassment, or disrespectful conduct toward others.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Plagiarise content (copy, use as their own, without citing the original creator) I find online.
- Post personally-identifying information, about myself or others.
- Agree to meet someone I meet online in real life.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to access sites, servers, accounts, or content that isn't intended for my use.