

Coláiste Chiaráin

Acceptable Use Policy

(2020 Draft V1)



Policy Statement:

Coláiste Chiaráin, Croom is committed to ensure that all users including students, staff and parents will benefit from the use of technology to enhance learning. This policy is in place to ensure technology is used in a safe, effective and appropriate manner.

Aims of this Policy:

- 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.

Table of Contents:

General Principles	2
General Rules	3
Passwords:	3
Content Creation, sharing and publishing:	3
Removable storage devices:	4
Activity Specific Rules	4
Internet / World Wide Web Use	4
Social Media and instant messaging	5
Email Accounts	5
Photo, Video and Voice recording	6
Desktop Computers in Labs	6
iPads	6
Chromebooks	7
Personal Devices (tablets, laptops):	7
Sanctions	8
Monitoring	8

1. General Principles

- Data security is everybody's responsibility.
- The schools 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 reserves the right to monitor school technology (hardware, software services) to
 - o Protect its lawful interests.
 - o Prevent and/or detect crime (in collaboration with relevant authorities).
 - o 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:
 - o Pornographic or sexually explicit material.
 - o Discriminatory and harassing behaviour.
 - o Tasteless material (such as depicting of injury, harassment or animal cruelty).
 - o Material or activity inciting hatred.
 - o 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.
 - o Education on the AUP and internet safety as part of the wellbeing curriculum.
 - o Safer internet day activities.
 - o CPD opportunities for teachers in the area of internet safety.
 - o 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).

Things to do

- ✓ Treat others with respect at all times.
- ✓ Respect the right to privacy of all members of the school community.
- ✓ Respect copyright and acknowledge creators when using online content and resources.
- ✓ Exercise care and common sense in your use of information technology.
- ✓ Refer to the glossary at the back if you need a definition of any term in this document.

Things not to do

- ✗ Anything illegal.
- ✗ Anything that contravenes this policy.
- ✗ Anything that harasses or intimidates individuals or groups.
- ✗ Anything that will harm the reputation of the School.

2. General Rules

Passwords:

- The school will provide you 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 users 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. 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 teacher 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. Activity Specific Rules

Internet / World Wide Web Use

- Use of the internet and world wide web is provided for school use. Reasonable personal use is permitted provided it is lawful, ethical and takes place during authorised breaks.
- 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.
- 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.
- Students are not permitted to use internet access through mobile networks or set up 'hotspots' that share the same. All devices must connect through the school wifi.

Things to do

- ✓ Use the school's internet connection for educational and career development activities only.
- ✓ Report accidental accessing of inappropriate materials to the teacher or TEL Coordinator.
- ✓ Sites that are blocked usually ask you to click on a particular section to fill in a request to have the site reviewed by the NCTE as appropriate for teaching purposes. Please use this method of getting sites unblocked as the TEL Coordinator has no control over unblocking sites

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.

Social Media and instant messaging

- 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

- ✓ Obtain permission and support from a teacher if you are entering a competition or engaging in school activities that can be promoted on social media.
- ✓ 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 of any student or teacher for the purposes of sharing on social media.

Email Accounts

- All students are provisioned with an email account at the start of first year.
- School email accounts should be used for school purposes only.
- School email accounts should not be used to register for personal services like social media accounts.
- 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.
- NB:** When applying for CAO or university applications students should use personal email accounts as their school account will not be active after they leave.

Things to do

- ✓ Add a subject line to your email so the receiver will know what it is about.
- ✓ Immediately report to the Principal 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.

Photo, Video and Voice recording

- Most photographs, video and voice recordings taken in school will be considered 'personal data' under GDPR legislation. Careful management of this content is vital.
- School equipment must be used for all photo, video and voice recording.
- Students are permitted to take photos and record video and voice only with specific permission of a teacher, and only with school equipment.
- Students are not permitted to use personal equipment for such recordings.

Things to do

- ✓ Obtain permission and equipment from a teacher when you need to take photos or make video/voice recordings.

Things not to do

- ✗ Never use personal devices, take photos, record video or voice.

Distance Learning

4. Device Rules

Desktop Computers in Labs

- Use the logon credentials provided.
- If somebody else has left their account logged in YOU MUST log them out.
- Do not install software on the computer without instruction to do so by a teacher.
- Store your data on Google Drive, data stored on desktops is not backed up.
- The school may audit computers to ensure compliance with this policy.

Things to do

- ✓ Log out of your accounts before leaving the computer.
- ✓ Save your data to google drive.
- ✓ Do not damage your computer

Things not to do

- ✗ Change settings on the computer (including wallpaper etc) without permission.
- ✗ Install software without permission.

iPads

- 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
- Do not change any of the settings on the device such as font size etc 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

Things to do

- ✓ Log out of all apps/accounts after use
- ✓ Don't use the camera without permission

Things not to do

- ✗ Record video without permission and supervision of teacher
- ✗ Use the camera without permission and supervision of teacher

Chromebooks

- Chromebooks are being provided to some students and sets of chromebooks are available for use by teachers.

Things to do

- ✓ Log out after use.

Things not to do

- ✗ Do not use the chromebook with someone else's account. Log them off and use your own credentials.
- ✗ Do not damage or mishandle the device.

Personal Devices (tablets, laptops):

- The school supports the use of personal devices (laptops, tablets) for the purposes of technology enhanced learning.
- Mobile phone use is detailed in a separate specific policy. Please Refer to the Mobile Device Policy.
- Students should use the school internet connection at all times.
- Personal devices should not contain any content that is deemed offensive or inappropriate as per the definition in the general principals.
- The school reserves the right to revoke permission for the use of personal devices where they have been found to, or suspected to be in breach of this policy.
- In order to ensure you are using the device for educational purposes a teacher may ask to view your screen at anytime and you will be required to show it
- The use of personal devices in the classroom is always at the discretion of the classroom teacher.
- The use of cameras and microphones on personal devices is prohibited.

Things to do

- ✓ Connect to the school network.
- ✓ Check with the teacher if it is appropriate to use your own device for the given task.

Things not to do

- ✗ Never use camera or microphone equipment on personal devices.
- ✗ Do not bring a device to school that contains offensive or inappropriate material.
- ✗ Use mobile data connections or hotspots.

Sanctions

- Sanctions will be applied in line with the schools disciplinary procedures.
- The severity of the sanctions will depend on the nature of the infringement.
- Any suspicion of illegal use of technology will be reported to an Garda Síochána.
- 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. In this case they will be expected to make alternative arrangements in relation to completing the task/coursework involved.
- Where it is found that students have intentionally damaged school equipment parents will be asked to cover the cost of the damage.

Monitoring

- The school will monitor traffic on our school network.
- Traffic that uses the internet is also monitored by the PDST for the purposes of filtering and legal compliance.
- Communication and activity on the schools G Suite services (email, document sharing etc) is logged.
- To investigate a suspected breach of this AUP the School Principal/Deputy Principals may liaise with the school TEL coordinator to access logs, files and email correspondence to investigate said breach.

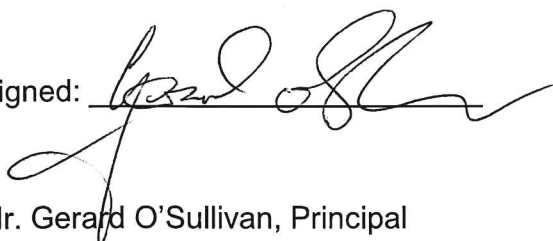
This policy was adopted by the Board of Management of Coláiste Chiaráin on **Tuesday 25th August, 2020.**

Related Policy Documents: Mobile Device Policy, review date - August 25th 2020.

Signed: 

Date: 25/08/2020

Mr. Tony Brazil, Chairperson, Board of Management

Signed: 

Date: 25/08/2020

Mr. Gerard O'Sullivan, Principal