Acceptable Use Policy
March 2025

THIS POLICY LINKS WITH:

Health and Safety Policy

Child Protection Procedures

Code of Behaviour

Anti-Bullying Procedures

DEVELOPMENT OF POLICY

March 2025	Initial review of policy – SMT & IT coordinator
March 2025	Review with IT team – Digital champions
March 2025	Consultation with Staff; Student Council; Parents Association/Group;
April 28th 2025	Finalisation of Draft and Input of Feedback for sending to Board of Management
Date	April 28th 2025 Policy Agreed by Board of Management
Policy Available for Staff at:	School Website
Policy Available for Parents at:	School Website

Context

The Management and Staff of PCH recognise that access to Information and Communication Technology (ICT), including the internet, gives our students enhanced opportunities to learn, engage, communicate and develop skills that will prepare them for many aspects of life. We expect students to use such technologies and the internet in a safe, ethical and responsible manner always and for educational purposes, both in school and off-campus. Use of digital technologies and internet should be conducted within the parameters of internet safety, the Acceptable Use Policy (AUP), student and staff well-being, and in an educational context. The Acceptable Use Policy has been developed following consultation between staff, parents, students, Principal and the Board of Management. In this policy document the term 'parent' is taken to include 'guardian'.

The Acceptable Use Policy outlines the guidelines and behaviours that our students are expected to follow when using their personal devices or school-owned devices / personal computers / recording equipment on the school campus, at school organised activities and in relation to off-campus use of devices. At all times Child Protection and Data Protection are of paramount importance in the implementation of this policy.

All members of the school community are expected to familiarise themselves with the contents of this policy.

Introduction

The aim of this Acceptable Usage Policy is to ensure that students, staff, and all users of the school's Information and Communication Technology (ICT) resources use these tools in a safe, respectful, and effective manner. This policy applies to the use of digital devices, internet access, school networks, email, and all online platforms used in the school context.

All students, teachers, and staff must adhere to this policy when using school-owned or personal devices, the internet, and other digital tools in the school environment. The goal is to promote a safe, respectful, and productive learning and teaching environment.

The aim of this Acceptable Usage Policy is to ensure that students, staff, and all users of the school's Information and Communication Technology (ICT) resources use these tools in a safe, respectful, and effective manner. This policy applies to the use of digital devices, internet access, school networks, email, and all online platforms used in the school context.

Scope

This policy applies to all members of the school community who have access to and use of the school's ICT systems and digital platforms, both on-site and remotely. This includes:

- Students
- Teachers
- Administrative staff
- Visiting professionals or contractors

Purpose

- To support effective teaching and learning through safe and responsible use of ICT.
- To protect all members of the school community from inappropriate or harmful online activity.
- To ensure compliance with the school's legal and safeguarding obligations.
- To guide proper use of school platforms, especially **Google Workspace for Education**, including **Google Classroom**.

Aims

The AUP aims to:

- Protect students from harmful content and online risks
- Promote responsible digital citizenship
- Ensure compliance with legal obligations, including the **General Data Protection Regulation (GDPR)** and **Child Protection Guidelines**
- Support teaching and learning through safe and appropriate ICT use

4. Guidelines for Acceptable Use

Students must:

- Use school ICT equipment only for educational and school-related purposes
- Respect others in all digital communications, refraining from inappropriate or offensive language
- Log in using only their assigned username and password
- Report any accidental access to inappropriate material to a teacher immediately
- Use school-approved platforms (e.g., Microsoft Teams, Google Classroom) under supervision
- Follow teacher guidance when using digital tools in the classroom
- Respect copyright and not plagiarise content

The aim of this Acceptable Use Policy is to ensure that students will benefit from learning opportunities offered by the school's digital technologies, portable technologies and internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school Acceptable Use Policy is not adhered to this privilege will be withdrawn and appropriate sanctions will be imposed, as per the Code of Behaviour. Internet access is intended for educational purposes and every reasonable precaution will be taken by the school to provide for online safety. However, the school cannot be held responsible if students access unsuitable websites or material, or use them inappropriately.

It is envisaged that school and parent representatives will revise the Acceptable Use Policy annually. The Acceptable Use Policy should be read carefully by parents and students so that the conditions of use are fully accepted and understood.

School's Strategy

The school will employ a number of strategies in order to maximise learning opportunities and reduce risks associated with the internet for students. These strategies are as follows:

General

- Internet sessions will be supervised by a teacher, where possible.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor students' internet usage.

- Students and teachers will be provided with training in the area of internet safety and digital literacy.

- 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 memory sticks/cards, personal USBs, CDROMs etc. is **not** permitted.

- The use of digital storage media (e.g. Cloud storage) in school requires teacher's advance permission.

- Students will always treat others with respect and will not undertake any actions that may bring the school into disrepute.

- Students may only access device applications when instructed by a teacher to do so. Students are forbidden from opening apps in class or going online, unless instructed to do so, and only for the purposes instructed by a teacher.

- Cyberbullying in any form is a very serious issue and will not be tolerated. Any report of cyberbullying will be taken seriously by the school management and appropriate investigative procedures followed, in keeping with the school's Anti-Bullying Policy.

- Host webinars or online seminars on cyberbullying and internet safety for parents.

Internet

- The school's internet access is provided by PDST NCTE (School-Filtered Broadband). The school's Wi-Fi will be available to all students and staff. The Wi-Fi is code protected for security reasons and to help ensure child and data safety. Students are not permitted to be informed of the code or to attempt to by-pass the code. No other networks / personal data (3G, 4G, Personal Hotspots etc.) may be accessed by students while on school grounds or as part of a school activity, unless under the direct instruction and supervision of a teacher.

- Students will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise explicit or objectionable materials.

- Students will report accidental accessing of inappropriate materials in accordance with school procedures.

- Students will use the internet for educational purposes only.

- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement). Students will be required to exercise care and attention in citing sources, references, photos / images and to acknowledge copyright if some material is used in their work. When downloading material from the internet,

students will take reasonable care to ensure that the material is from safe sources, copyright-free (where possible) and referenced appropriately.

- Students will never disclose or publicise personal information in relation to themselves or others.

- Downloading by students of materials or images not relevant to their studies is in direct breach of this Acceptable Use Policy.

- Students 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.

- School computers will be available to students. At all times, students must use their school login details and their own storage area on the school Google Drive.

- It is strictly forbidden for students to delete the work or files of other students. It is strictly forbidden for any student to attempt any act of hacking or other form of sabotage that could compromise the security of the school's network and digital data. Any such action will result in a serious sanction being imposed, including the option to suspend or expel the student involved.

- Students must log out of their own accounts at the end of each internet session. Students are not permitted to access the school accounts of other students. In the event where a student accesses a school device and finds another student has not logged out, the student accessing the device must log the other student out before proceeding to use the device. The student should also inform the relevant teacher.

E-mail

- Students will use approved school e-mail accounts under supervision by or permission from a teacher.

- Students will not send or receive any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person.

- Students will not reveal their own or other people's personal details, such as addresses, telephone/mobile phone numbers or pictures.

- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.

- Students will note that sending and receiving e-mail attachments is subject to permission from their teacher.

- Students will use their school email account for educational use, and will not use their personal email accounts to communicate with teachers.

Social Media / Internet Chat

- Students will only have access to chat rooms, discussion forums, messaging 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 be supervised, where possible.
- Face-to-face meetings with someone organised via internet chat will be forbidden.
- Only official school social media accounts, or social media as instructed by a teacher, may be accessed by students on school grounds or as part of a school activity. Students' personal social media accounts may not be accessed during the school day or using the log-in details ascribed by the school.
- Students will not attempt at any time to connect with any member of staff on that staff member's own personal social media account(s).

School Website / Media Accounts

- Students will be given the opportunity to publish projects, artwork or schoolwork on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website /media accounts.
- The website / media accounts will be regularly checked by the relevant co-ordinating teachers to ensure that there is no content that compromises the safety of students or staff.
- The publication of student work will be coordinated by a teacher.
- Students' work will appear in an educational context on web pages with a copyright notice prohibiting the copying of such work without express written permission.
- The school will endeavour to use digital photographs, audio or video clips focussing on group activities. Content focussing on individual students will not be published on the school website without parental permission. Video clips may be password protected.
- The school's ICT co-ordinator (or another person designated by the Principal) will take a photograph of each student for the student's Tyro account.
- It is considered a serious breach of this policy for a student or member of staff to create and/or use a fake social media account.

Recordings

- Only recordings permitted by a teacher are allowed. Students are forbidden from using any device to make an unauthorised recording of any sort in class, on a school outing or as part of a school activity.

- Students are forbidden from taking photos, video or sound recordings of anyone in the school (including students, staff, parents and visitors) unless instructed by a teacher to do so, and even then, only with the consent of the individual(s) involved. Students must not share such material online without the clear permission of a teacher and only for educational or school promotional purposes.

- Students may be digitally recorded for educational purposes throughout their time in PCH. Such purposes include Classroom-Based Assessments (CBAs), Leaving Certificate Vocational Programme (LCVP/Links Module), extra-curricular activities and participation in educational activities and outings.

- Recordings will be made on school devices and reasonable care will be taken to store recordings securely on the device and on the school's network. This includes both subject-related recordings and recordings of extra-curricular activities in which students are engaged.

- Some recordings will be brought to Subject Learning and Review (SLAR) meetings by teachers in order to discuss and determine appropriate grade descriptors. Where it is necessary to store such recordings on portable devices such as USB keys or external hard drives, reasonable care will be taken by teachers to ensure the safe-keeping of such recordings. Where cloud storage is used, this will be secure cloud storage and school-approved.

- All recordings will take place in cognisance of the Child Safeguarding Statement and Child Protection Procedures and will be in line with the Acceptable Use Policy.

- While most recordings will be deleted soon after a SLAR meeting, some recordings may be stored for a period of up to seven years and used for educational purposes (e.g. demonstration of descriptor examples of highly effective practice).

- Recordings (e.g. photographs, short video clips) may also be used for promotional purposes of the school, e.g. via the school's official social media accounts. Reasonable care will be taken by teachers to ensure that recordings used for demonstration

purposes, or shared via social media, are appropriately consented to by the student(s) involved.

- Any parent or student who does not wish for a recording (including photographs) of the student to be made or shared within the school for educational purposes, must so inform the Principal in writing. Students must notify the relevant teacher in such situations, in advance of any recording being made or shared.

Personal Devices

- Students may store their mobile phones securely in their school bags / lockers / pockets but they must be powered off throughout the school day (including before school starts, break times and after school), unless a teacher requests a student to use their phones for educational purposes. Once such sessions are finished, student mobile phones must again be powered off and returned securely to school bags / lockers / pockets. Students are not permitted to have a mobile phone powered on in 'Silent' and/or 'Vibrate' mode – mobile phones must be fully powered off while on school grounds.

- Students using their own technology in school, such as using a mobile phone in school without a teacher's explicit permission, sending nuisance text messages, or the unauthorised taking of images with a mobile phone camera still or moving, are in direct breach of this Acceptable Use Policy and the school's Code of Behaviour. Sanctions may be applied in such cases, as per the school's Code of Behaviour. Use of cameras on digital devices is only permitted with a teacher's permission. Where a phone is confiscated by a teacher it will be given to the office for safe-keeping and return to the student at the end of the school day. The infringement will also be recorded on a 'purple sheet' by the teacher who confiscated the phone. A sanction may apply at the discretion of the relevant Year Head. Students will be reminded of responsible device use and sanctions for misuse from time-to-time via the school intercom and at Assemblies.

- Students must take care of their mobile devices and not leave them unattended.

- Students will ensure that screensavers are appropriate. Screensavers of an inappropriate nature (e.g. obscene, hateful, sexual, objectionable, defamatory) will not be permitted on school or personal devices.

- Student devices, including mobile phones, must be powered off and stored in students' school bags while an exam is taking place or left in a box at the top of the examination centre.

- In certain circumstances it may be necessary for a teacher / school management to inspect a student's device (e.g. where there are reasonable grounds to believe that the student has not complied with this policy).

- Irresponsible or unethical use of mobile devices or the internet will be considered a serious infringement of the Code of Behaviour and disciplinary action will be taken where this applies.

- Smart watches are not permitted while on school grounds.

- 'Airdrop' must be switched off all student devices while on school premises. Students are not permitted to use 'Airdrop' while on school premises.

Staff

- Staff will model good practice and ethical, responsible use of digital technologies and the internet with students.

- In keeping with the Teaching Council's Code of Professional Conduct, staff will ensure that any communication with students, colleagues, parents and others is appropriate, including communication via electronic media, such as e-mail, texting and social media [par.3.7].

- Staff should ensure that the privacy settings on their social media accounts are robust. Reasonable care should be exercised not to allow any social media communication with students using their personal social media accounts, personal e-mail accounts or personal mobile phones. Staff and students are permitted to communicate for educational purposes via the official school's social media accounts. Personal mobile numbers, email addresses or social media details should not be shared by teachers with students. Teachers should not 'Friend' students on social media platforms or accept a Friend request from a student on the teacher's personal social media account. Staff will only use their professional email (not personal email) addresses and school accounts to communicate with students and parents.

- All social media accounts that claim to represent the school's activities must first be approved by the Principal by the teacher overseeing the activity. The teacher will ensure that a trustworthy person (either the teacher or a student) is nominated to monitor the account. Staff will comply with agreed procedures for the setting up and monitoring of school-approved social media accounts.

- Staff must ensure that they do not knowingly access, download or otherwise have in their possession while engaged in school activities, inappropriate materials/images in electronic or another format [par 3.8].

- School devices used by staff are for school business only. Staff will not store personal data on school devices.

- Staff will take reasonable care of digital devices on which student data can be accessed, and endeavour to protect student data securely. Devices must be password-protected, have 2-Step Verification and stored securely. Particular care will be taken by staff to log out of the data management system (Tyro) after each session, and out of their G-suite account on school devices.

- Staff will not disclose the Wi-Fi code to students or parents.

- Staff will familiarise themselves with relevant Department of Education and Skills circulars pertaining to the use of digital technologies.

Parents

- As the primary educators of children, parents are encouraged to be positive role models in their use of social media platforms, in order to foster good example for their children. Parents are advised against using social media in ways that are not supportive of the school or its policies. We encourage all parents to use social media for positive and ethical purposes to promote the good name of the school and of the school community.

- Parents are respectfully reminded of their responsibilities to supervise their children's internet access and use at home, and to ensure that adequate parental controls are in place to reduce the risk of children accessing inappropriate material.

- Since there is no appeals process for descriptors awarded to students for their Classroom Based Assessments, the decisions of the subject departments are final.

- Parents are advised to familiarise themselves with support materials for parents on www.webwise.ie and follow the guidance given therein.

- Any parent or student who does not wish for a recording (including photographs) of the student to be made or shared for educational purposes, must so inform the Principal in writing. Students must notify the relevant teacher in such situations, in advance of any recording being made or shared. Any parent who has a concern in relation to any aspect of this policy should contact the Principal in writing. Any parent who wishes to withhold consent to the above must indicate this in writing to the Principal and an appointment will be made with a member of the senior management team to discuss the concern.

Legislation

The school will provide information on the following legislation relating to use of the internet which teachers, students and parents should familiarise themselves with, through the following links:

- Data Protection Act 1988 and Data Protection Amendment Act 2003 http://www.irishst
- Child Trafficking and Pornography Act 1998
- Non-Fatal Offences Against the Persons Act 1997
- Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993
- Video Recordings Act 1989

Data Protection and Privacy

- All users must respect the privacy of others and adhere to the principles of the **GDPR**.
- Users must not access, download, store, or share personal data without authorisation.
- Photographs or videos of students may only be taken and shared with parental consent and for school-related purposes.

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the internet. Several sites and national bodies offer helpful advice to parents, particularly with respect to how they can best monitor their child's use of the computer at home. Important and useful information can be found on the following sites:

www.webwise.ie, www.internetsafety.ie, www.education.ie, www.thinkb4uclick.ie, www.bully4u.ie

Sanctions

Misuse of the internet or other personal devices may result in disciplinary action as per the school's Code of Behaviour The school also reserves the right to report any illegal activities to the appropriate authorities.

- **Disciplinary Action**: Violations of the AUP may result in disciplinary actions, including loss of technology privileges, detention, suspension, or expulsion.
- **Legal Consequences**: Any illegal activity, such as hacking, harassment, or plagiarism, may result in legal consequences.

The use of technology in the classroom is a privilege, not a right. It is important that all users understand and respect the terms of this policy to create a positive and secure environment for learning and teaching. Violations of the AUP undermine the integrity of the school community and will not be tolerated.

The attendance by students in this school implies acceptance by them and their parents of this Acceptable Use Policy.

Reviewed and ratified by the Board of Management on: April 28th 2025
Date of next review: April 2026.

Signature (Chairperson): _____

For and on behalf of the Board of Management