



Castleisland Community College

ICT Acceptable Use Policy – 2026



Introductory Statement

This policy sets out the acceptable, safe and responsible use of information and communication technology in Castleisland Community College. It applies to students, staff, parents and guardians, approved visitors and any person using school ICT systems, accounts, networks or devices for school-related purposes.

The school uses digital technology to support teaching, learning, assessment, communication and administration. Access to these resources brings responsibilities. Users must protect their own safety and privacy, respect others, care for equipment, follow staff instructions and use technology lawfully and for appropriate educational or professional purposes.

This policy covers school-owned equipment, school accounts and services, the school network, devices bought through the school laptop purchase scheme, and privately owned devices permitted under the traditional Bring Your Own Device (BYOD) arrangement. It applies in school, during school activities and, where relevant, to off-site online behaviour that affects members of the school community or the orderly operation of the school.

2 Guiding principles

- Use ICT primarily to support teaching, learning, assessment, administration and school communication.
- Treat other users respectfully and do not use technology to harm, intimidate, embarrass, harass or exclude another person.
- Protect personal information, passwords, accounts and confidential school information.
- Respect copyright, licences and intellectual property, and acknowledge sources appropriately.
- Take reasonable care of school-owned and student-owned equipment.
- Follow the direction of teachers and other authorised staff when using devices or online services.
- Report accidental access to inappropriate material, suspected security incidents, harmful content or online bullying promptly to a member of staff.

3 Education for safe and responsible use

Digital citizenship, online safety, media literacy and responsible use of technology will be addressed through relevant subject areas, Digital Media Literacy, SPHE, guidance and other school programmes. The school may also provide information or workshops for students, staff and parents or guardians and will mark Safer Internet Day or related initiatives where appropriate.

4 Legal and policy framework

This policy should be read in conjunction with current Irish and European law and relevant Department of Education procedures, including data protection, copyright, child protection, online safety and bullying requirements. Relevant legislation and guidance include:

- the General Data Protection Regulation and the Data Protection Act 2018;
- the Copyright and Related Rights Act 2000, as amended;
- the Child Trafficking and Pornography Act 1998, as amended;
- the Harassment, Harmful Communications and Related Offences Act 2020;
- the Online Safety and Media Regulation Act 2022; and
- Bí Cineálta Procedures to Prevent and Address Bullying Behaviour for Primary and Post-Primary Schools.

This list is not exhaustive. The school will apply the law and official guidance in force at the time of an incident or review.

5 School accounts network and internet access

- Each user must use only the account issued or authorised for them. Accounts and passwords must not be shared, except where an authorised shared account has been established for a specific school purpose.
- Users must use strong passwords, keep them confidential and notify the school promptly if an account may have been compromised.
- School accounts, including Microsoft 365 services such as Outlook, Teams and OneDrive, are for educational or professional school use.

- Students may access the internet and school digital services only as directed or permitted by a teacher or authorised staff member.
- Users must not deliberately access, create, store, send or share illegal, obscene, hateful, threatening, defamatory or otherwise inappropriate material.
- Users must not attempt to bypass filtering, security controls or access restrictions, including through proxy services, VPNs, personal hotspots or mobile data where these are prohibited by the school.
- Downloading or uploading unusually large files is permitted only where required for school work and authorised by a staff member.
- Users must not introduce malware, interfere with the network, attempt unauthorised access, probe for vulnerabilities or alter another person's files or settings.
- The school may block or restrict websites, applications, downloads or services where this is necessary for safety, security, legal compliance or the effective operation of the network.

6 Student devices two available routes

Castleisland Community College supports both a school laptop purchase scheme and a traditional BYOD arrangement. In both cases the device is normally owned by the student or family, but the route by which it is obtained and the technical standards may differ.

6.1 School laptop purchase scheme

Students participating in the laptop purchase scheme obtain a school-recommended laptop that meets specified educational and technical requirements. Participation in the scheme does not transfer ownership or responsibility for the device to the school.

- Students and parents or guardians are responsible for the device's care, safe transport, charging, maintenance, insurance and repair, subject to any separate warranty or maintenance arrangement supplied with the purchase.
- The device must be brought to school on designated days, fully charged and ready for use.
- Required security, management, filtering and educational software must not be removed, disabled or deliberately interfered with.
- The device must be used in class only when and as directed by the teacher.
- The student must comply with all provisions of this AUP while using the device, whether in school or for school-related work elsewhere.

6.2 Traditional Bring Your Own Device

Where the school permits traditional BYOD, a student may bring an independently purchased laptop or tablet for school work. The school determines which device types, operating systems and minimum specifications are suitable. Permission may be limited to particular year groups, subjects, activities or periods.

- A BYOD device must be capable of accessing the required school platforms and must have current system and security updates.
- The student and parent or guardian remain responsible for purchase, compatibility, mobile data costs, care, charging, maintenance, insurance, repair and replacement.
- The school cannot guarantee technical support, network access or compatibility for every privately sourced device.
- A student may not connect a device to the school network or use it during school time unless the school and the relevant teacher permit this.
- Mobile phones, smartwatches and personal gaming devices are not treated as general BYOD learning devices. Their possession and use are governed by the school's separate mobile phone and personal electronic devices rules.

6.3 Rules applying to both routes

- Devices must be used for learning and school-related purposes during school time. Gaming, social media, entertainment and unrelated communication are not permitted unless a teacher expressly authorises a particular educational use.
- Students must connect through the school-approved network and may not use personal hotspots or mobile data to bypass school controls.
- Students must not access another person's device, account or files without permission.
- Students must not install unauthorised software or change settings in a way that creates a security, safeguarding or network risk.
- The school is not responsible for loss, theft or accidental damage to a privately owned device, except where liability arises under law.

- The school may direct that a device be closed, put away, surrendered temporarily or removed from the classroom where its use is unauthorised, disruptive or may preserve evidence of a serious incident. Any such action will follow the Code of Behaviour and applicable school procedures.

7 Monitoring privacy and inspection

The school may monitor and retain activity carried out through school accounts, services, devices and networks in accordance with its data protection obligations and for legitimate purposes such as safeguarding, cybersecurity, technical administration, investigating suspected misuse and maintaining the effective operation of school systems.

Use of a personal device on the school network does not give the school an unrestricted right to inspect all private content on that device. Where there is a reasonable concern about a breach of school policy, safeguarding, cybersecurity or law, the school may ask the student to display relevant content or settings and may temporarily retain the device where permitted under school procedures. Any examination will be necessary, proportionate, limited to the concern, and carried out by an authorised person. Parents or guardians and An Garda Síochána or another statutory authority may be involved where appropriate.

8 Email Teams messaging and online communication

- School email, Teams and other approved communication systems must be used respectfully and for school-related purposes.
- Users must not impersonate another person, send spam, forward chain messages, or circulate harmful, misleading or inappropriate content.
- Students must not use instant messaging or social media during school time unless a teacher has authorised a specific educational activity.
- Students must not seek to connect with staff through staff members' personal social media accounts. School communication should take place through approved channels.
- Users must consider the audience, accuracy, tone, confidentiality and permanence of any digital communication before sending or posting it.

9 Images video audio and recordings

- Students may photograph, film or record during a lesson or school activity only with the express permission of the supervising teacher and the people being recorded.
- No user may secretly record a student, staff member, visitor, meeting, lesson or school activity.
- Images, recordings or student work must not be posted, forwarded, altered or published without appropriate permission.
- Staff should use school-approved equipment, accounts and storage for recordings involving students wherever practicable and must follow the school's data protection and child safeguarding procedures.
- The school may publish images, recordings and student work on approved school channels where the necessary consent or other lawful basis is in place. The school will avoid unnecessary identifying information.

10 School website and official social media

The school website and official social media channels are managed under the authority of the Board of Management by authorised staff. They may be used to share school information, notices, learning activities and achievements. Only authorised persons may publish on behalf of the school. Personal views must not be presented as the views of Castleisland Community College.

11 Artificial intelligence

Artificial intelligence may support learning and work when used transparently, critically and with teacher or school approval. It must not replace a student's own thinking, learning or authorship.

- Students may use only AI services approved by the school, suitable for their age and permitted by the teacher for the particular task.
- Students must follow the teacher's instructions on whether and how AI may be used in homework, assessment, CBAs, projects or examination-related work. Presenting AI-generated work as one's own may be treated as academic dishonesty.
- Where required, users must acknowledge meaningful AI assistance and describe how it was used.
- AI output must be checked for accuracy, bias, fabricated information, unsafe advice and inappropriate content. The user remains responsible for submitted or published work.

- Personal data, confidential school information, assessment material, photographs, recordings or identifiable student work must not be uploaded to an AI service unless the school has specifically approved the service and the use.
- AI must not be used to impersonate, deceive, bully, create harmful or sexualised material, produce deepfakes, evade school safeguards or undermine another person's privacy or intellectual property.
- Staff use of AI must comply with data protection, child safeguarding, copyright, professional judgment and assessment requirements.

12 Bullying and harmful online behaviour

Bullying behaviour, including cyberbullying, will be addressed under the school's Bí Cineálta policy and procedures. Online conduct may fall within the school's remit where it occurs in school, during school activities, through school systems, or where off-site conduct has a clear impact on a student's participation in school or on the school community.

- Users must not use digital technology to threaten, harass, humiliate, exclude, defame or target another person.
- Harmful material must not be liked, reposted, forwarded or otherwise amplified.
- Students should preserve relevant evidence and report concerns to a trusted adult or member of staff rather than responding or retaliating online.
- Immediate risks to a child or other person will be managed through the school's child safeguarding and emergency procedures.

13 Parents and guardians

- Parents and guardians should discuss this AUP with their child and support compliance with school rules.
- They are responsible for supervising their child's use of privately owned devices and online services outside school and for respecting platform age requirements.
- Parents and visitors must not photograph, record or publish identifiable images of other students or staff at school events without appropriate permission.
- Concerns about online behaviour should be reported through appropriate school channels and should not be pursued through public social media posts.
- Parents and guardians should notify the school promptly about a lost device, compromised school account or online incident that may affect their child or the school community.

14 Staff and authorised visitors

- Staff and authorised visitors must use school ICT, accounts and networks for legitimate professional or approved purposes and protect passwords and confidential information.
- Staff must use their school-issued email account for professional school communication and must not use it to create personal or social media accounts.
- Student internet and device use must be appropriately supervised, taking account of student age, needs, activity and risk.
- Network, administration, VMware and other privileged credentials must not be disclosed to students or unauthorised persons.
- Staff must use approved storage and sharing arrangements for personal data and must report suspected data breaches, phishing, malware or account compromise promptly.
- Personal use of school ICT must be limited, reasonable, lawful, secure and must not interfere with work or expose the school to risk.
- Teaching practice students, work-experience participants, visitors and outside agencies may use school facilities only with authorisation and must follow this AUP and relevant confidentiality requirements.
- Staff must maintain appropriate professional boundaries and manage personal social media privacy and professional reputation carefully.

15 Breaches sanctions and reporting

A breach may result in one or more proportionate actions under the Code of Behaviour, staff procedures or other relevant school policy. Actions may include instruction or support, a warning, contacting parents or guardians, temporary restriction or withdrawal of account, network or device privileges, temporary retention of a device, restorative or disciplinary measures, or referral to the Board of Management.

Serious, repeated, illegal or safeguarding-related conduct may be reported to relevant authorities or services, including An Garda Síochána, Tusla or the Data Protection Commission, as appropriate. The school may preserve relevant records or evidence in accordance with law and school procedures.

16 Linked school policies

- Code of Behaviour and suspension and expulsion procedures
- Bí Cineálta policy to prevent and address bullying behaviour
- Child Safeguarding Statement and Risk Assessment
- Data Protection Policy and Privacy Notices
- Mobile Phone and Personal Electronic Devices Policy
- Assessment, academic integrity and relevant subject or programme procedures
- Staff ICT, social media, communications and records-management procedures, where applicable

17 Review and ratification

The Digital Learning Team and school management will keep this policy under review in consultation with staff, students, parents or guardians and the Board of Management, as appropriate. It may be amended in response to changes in technology, school practice, legislation, Department of Education guidance or identified risk.

This policy was ratified by the Board of Management on 22nd September 2026

Signed: Jim Kelly

Chairperson, Board of Management

Signed: Hatred Connell

Principal

Date: 22/9/26

Appendix 1 Student and Parent Guardian Agreement

This agreement applies to use of school ICT and to student-owned devices used under either the school laptop purchase scheme or the traditional BYOD arrangement.

Student declaration

I have read, or had explained to me, the ICT Acceptable Use Policy. I understand that I must use school technology, accounts, networks and permitted personal devices responsibly and follow staff instructions. I understand that breaches may result in restrictions and other actions under school policy.

Student name: _____

Student signature: _____ Date: _____

Parent guardian declaration

I have read and discussed the ICT Acceptable Use Policy with my child. I understand the responsibilities that apply to school systems and to any student-owned device used under the laptop purchase scheme or traditional BYOD arrangement. I will support my child in complying with the policy and will contact the school if I have a relevant concern.

Parent or guardian name: _____

Parent or guardian signature: _____ Date: _____