Cambridge House Grammar School

Code of Practice for Safe and Effective Use of Digital Technologies (including Bring Your Own Devices - BYOD)

Updated 2025

Introduction

This Code of Practice has been revised in accordance with the Department of Education's current *Acceptable Use of ICT in Schools* guidance (2025) and updated e-Safety Frameworks. It reflects C2k/NICET developments and aligns with the latest *Empowering Learners* digital strategy.

The safe, responsible, and effective use of the internet, email, mobile technologies, and digital devices is essential in education. All users must comply with legislation related to data protection, copyright, online safety, privacy, cybercrime, and equality.

As part of the Northern Ireland Curriculum, pupils are expected to develop digital literacy skills to locate, retrieve, evaluate, and exchange information safely. Teachers must actively integrate digital tools into learning. ICT remains a vital lifelong skill for education, employment, and personal development.

Purpose of Internet Use in School

1. Raise educational standards and pupil achievement.
2. Support staff professionalism and school operational systems.
3. Foster digital citizenship and 21st-century learning skills.
4. Provide equitable access to digital resources and experiences.

Roles and Responsibilities

Internet and technology safety is a shared responsibility between staff, leadership, governors, parents, and pupils.

All Users Must:

- Use digital tools legally, ethically, and respectfully.
- Follow the school's Acceptable Use Policy (AUP).
- Understand that monitoring and filtering systems are in place.
- Refrain from accessing harmful, illegal, or disruptive content.

Staff Expectations:

- Use school email and platforms for professional purposes only.
- Model responsible digital behaviour.
- Guide pupils in safe and educational online activity.
- Avoid bringing the school into disrepute via digital communications or social media.

Pupil Expectations:

- Understand digital access is a privilege, not a right.
- Use internet and digital tools responsibly.
- Avoid misconduct (see prohibited behaviours below).
- Comply with all school policies regarding e-safety and device use.

Prohibited Use Includes (but is not limited to):

- Accessing or distributing offensive, obscene, or harmful material.
- Using discriminatory or abusive language.
- Cyberbullying or harassment.
- Bypassing network security or filtering.
- Sharing passwords or accessing others' accounts.
- Infringing copyright or intellectual property rights.
- Using devices for unapproved commercial purposes.

Supervision and Monitoring

- Internet access is filtered and monitored by C2k and school administrators.
- Supervision is provided during digital activity, though independent research may be permitted with prior approval.
- Privacy is respected, but school systems (including C2k storage and email) are subject to inspection.
- Lessons on online safety and digital citizenship are embedded in the curriculum and pastoral care.

Examples of Acceptable Use Includes:

- Curriculum-related research and collaboration.
- Email communication under staff supervision.
- Learning-based interaction with approved platforms (e.g., Google Workspace for Education, Microsoft 365, etc.).

- Exploring careers and educational opportunities.

Examples of Unacceptable Use Includes:

- Gaming, unless part of curriculum.
- Subscribing to services or making online purchases without approval.
- Accessing social media or streaming services without permission.
- Sharing personal information online.
- Using anonymous or proxy browsing tools.

Pupils who are found to have been engaging in unacceptable use will be held accountable and be sanctioned in line with schools Behaviour for Learning Policy.

Cyberbullying and Online Abuse

Cyberbullying remains a serious concern in 2025. The school enforces zero tolerance for any such behaviour.

Cyberbullying May Involve:

- Abusive texts, emails, or messages.
- Misuse of social media platforms (e.g., TikTok, Snapchat, Instagram).
- Manipulating or sharing images without consent.
- Using online games to harass or intimidate.
- Sexting or sharing explicit content.

Pupils and staff are encouraged to report any incident immediately. The following laws may apply:

- Harassment Order (NI) 1997
- Malicious Communications (NI) Order 1988
- The Online Safety Act 2023 (UK)
- The Communications Act 2003

All incidents are recorded in pastoral systems and investigated consistently.

Parental Guidance

Parents play a vital role in reinforcing safe and responsible online behaviour at home.

Parents Are Advised To:

- Discuss online safety and digital rules with their children.
- Supervise internet use at home, particularly for younger pupils.

- Be aware of platforms and apps used by their children.
- Prevent the sharing of personal or financial information online.
- Report any threats, abuse, or suspicious activity to the school or PSNI.

The school provides up-to-date guidance through newsletters, information evenings, and its website.

Bring Your Own Device (BYOD) – 2025

Mobile phones, tablets, and other personal digital devices are now recognised as learning tools.

Accessing the School Wireless Network:

Pupils may connect to the secure guest Wi-Fi by:

1. Connecting to **C2kGuest**.
2. Accepting the AUP terms via browser.
3. Logging in with C2k credentials.
4. Installing *SmartConnect* for secure access.

First-time setup requires installation; ongoing access only requires login.

BYOD Guidelines

- Personal devices are permitted at teacher discretion only.
- Devices must be used for educational purposes during school hours.
- Messaging or contacting others is not permitted without permission.
- Use of personal devices must not distract others or disrupt learning.
- Photos or videos must never be taken or shared without consent.
- Use outside the classroom is only allowed under supervision or on trips.
- Attempting to bypass filters or security is strictly forbidden.

Consequences for Misuse

- Network access revoked.
- Device confiscation (returned to pupil or guardian).
- Ban on device use on-site or on trips.
- Disciplinary action per the Behaviour and Discipline Policy.

School Liability Disclaimer

Pupils bring personal devices at their own risk. The school is **not responsible** for:

- Damage to devices on school property.
- Lost or stolen devices.
- Charging, maintenance, or software issues.

Pupils must take full responsibility for securing and managing their own devices.

Annual Review

This policy will be reviewed annually by the SLT, ICT Coordinator, and Governors to ensure compliance with legal updates and best practice in digital safeguarding.

Policy updated 2025