



Kildare Town Community School

Acceptable Use Policy

Policy Title	Acceptable Use Policy (AUP)
Version	2.0
Date of Review	May 2026
Next Review Date	May 2028
Related Policies	Anti-Bullying Policy; Code of Behaviour; Child Safeguarding Statement; GDPR/Data Protection Policy; Social Media Policy; Remote Learning Policy

Introduction

Kildare Town Community School (KTCS) is committed to ensuring that all users — including students, staff, parents/guardians, and other authorised users — benefit from the learning opportunities offered by the school's Information Technology (IT) systems in a safe, effective, and appropriate manner. This policy is mindful of the need to bring the key components of the school's mission statement — Illuminate, Love, Serve — into the daily lives of all who work and learn in the school.

1. Rationale, Aims & Definitions

An educational goal of this school is to promote and maintain a culture of digital citizenship and cyber-safety that is in keeping with our school values and with legislative and professional obligations. Internet use and access is considered a school resource and privilege. If this Acceptable Use Policy (AUP) is not adhered to, this privilege will be withdrawn and appropriate sanctions — as outlined in this document — will be imposed.

An Acceptable Use Policy is a document that addresses all rights, privileges, responsibilities, and sanctions associated with all ICT usage in the school context. All users of our ICT infrastructure are responsible for ensuring that devices and systems are used in an effective, efficient, and ethical manner for educational purposes. This document establishes the rules and restrictions — including what is prohibited — that define acceptable use. Where deliberate misuse occurs, sanctions in accordance with the school's Code of Behaviour and relevant statutory law apply.

The purpose of internet use in Kildare Town Community School is to enhance learning through digital technologies, which is central to the Digital Strategy for Schools to 2027 and embedded in subject specifications for both Junior Cycle and Leaving Certificate. The internet also supports the professional work of staff and the management and administration of the school.

Key Terms in this Document

Term	Definition
Cyber-safety	Promoting safe use of the internet and protection against online threats, fraud, and harmful content.
Cyberbullying	Bullying that uses electronic communication — including social media, messaging apps, email, SMS, or online platforms — to intimidate, threaten, or harm another person.
ICT (Information and Communication s Technology)	Technologies that provide access to information through telecommunications and digital systems.
School's ICT Infrastructure	The school's computer network, internet access, telecommunications systems, computer software, cloud storage and communications platform (Google Workspace for Education), computers, and all other ICT equipment.
ICT Equipment	Includes desktop computers, monitors, keyboards, mice, portable devices, webcams, microphones, speakers, projectors, cameras, recording devices, external storage (USB/flash drives), visualisers, printers, photocopiers, scanners, mobile phones, Wi-Fi access points, the school server, and all associated cabling and wiring.
Digital Learning	The embedding of digital technologies within learning, teaching, and assessment practices.

Digital Technologies	Electronic tools, systems, devices, and resources that generate, store, or process data, including online learning platforms, software applications, and AI-assisted tools.
Inappropriate Material	Material dealing with matters of sex, cruelty, or violence in a manner injurious to children or incompatible with a school environment, as well as content promoting extremism, illegal activity, or self-harm.
Electronic/Cyber Crime (e-Crime)	Any criminal activity in which the internet or an electronic device is used to commit, target, or facilitate an offence.
Artificial Intelligence (AI) Tools	Software systems that simulate human intelligence processes, including AI-generated text, image, audio, or video tools (e.g. ChatGPT, Google Gemini, Canva AI, and similar platforms).
Generative AI	AI tools capable of producing text, images, code, audio, or video content in response to user prompts.
Personal Device	Any device owned by a student, staff member, or third party, not issued by the school.
BYOD (Bring Your Own Device)	A practice where users bring personally owned devices for educational use, subject to school approval and conditions.

2. Scope of this Policy

This policy applies to all users of the ICT infrastructure of Kildare Town Community School, including:

- All students (Junior Cycle and Senior Cycle)
- All teaching and non-teaching staff
- Parents/guardians accessing school systems
- Visitors, contractors, and other authorised users

This policy applies to:

- Use of school-owned ICT equipment on-site and off-site
- Use of the school network, Google Workspace for Education, and Vsware
- Use of personal devices connected to the school network or used for school purposes
- All online activity undertaken in a school context, including remote or blended learning

This policy must be read in conjunction with all other school policies. All policies are published on the school website.

Legislative Framework

This policy operates within the following legislative framework:

Legislation	Relevance
Education Act, 1998	School governance, student welfare
Data Protection Act, 1988 & Amendment Act, 2003	Personal data handling
General Data Protection Regulation (GDPR), 2018	Data protection, consent, student data rights
Data Protection Act, 2018 (Irish implementing legislation)	Domestic GDPR application
Freedom of Information Acts, 1997–2014	Access to records
Video Recordings Act, 1989	Recording and distribution of video content
Interception of Postal Packets and Telecommunications Messages Act, 1993	Monitoring of electronic communications

Child Trafficking and Pornography Act, 1998 (as amended)	Protection from online sexual exploitation
Education Welfare Act, 2000	Student attendance and welfare
Equal Status Acts, 2000–2018	Non-discrimination in educational access
Employment Equality Acts, 1998–2015	Staff equality and dignity
Children First Act, 2015	Mandatory reporting, child safeguarding
Criminal Justice (Offences Relating to Information Systems) Act, 2017	Cybercrime offences
Online Safety and Media Regulation Act, 2022	Online safety obligations, harmful online content
Copyright and Related Rights Act, 2000	Intellectual property and fair use
Non-Fatal Offences Against the Person Act, 1997	Harassment via electronic means
Child Protection Guidelines for Post-Primary Schools (DES, 2017)	Safeguarding in a school context

3. Use of and Access to Digital Technologies & ICT Resources

3.1 School ICT Facilities

KTCS provides the following ICT resources:

- Two computer rooms, laptop trolleys used
- One multimedia room, laptop trolley used
- Two class sets of laptops (rotational timetable)
- A desktop computer, digital projector, and internet access in each classroom
- At least one laptop per subject department (Junior Cycle) for CBA support
- Google Workspace for Education accounts for all staff and students
- Separate network provided for students and guest devices. Students do not have permission to connect to the school devices or admin and teachers network
- Individual network login for all staff and students
- Remote Management Software is installed on all school devices by the managed Service Provider
- Senior Cycle redevelopment - 5th Year students will have the opportunity to purchase a Google chrome device supported through a payment plan option. This is necessary as students will now complete Additional Assessment Components (AACs) across a range of subjects.

Access to shared computing resources operates on a rotational timetable managed by the relevant subject teacher.

3.2 Health & Safety Considerations for Use of ICT

- Computer rooms are fitted with appropriate workstations providing adequate space for comfortable use.

- Students are encouraged to maintain good posture when using ICT equipment.
- No eating or drinking is permitted near ICT equipment.
- Trailing cables are secured; bags are stored under desks to prevent trip hazards.
- Flammable materials are kept away from all ICT equipment.
- Computer rooms are ventilated regularly.
- All school devices are powered off at the end of the school day.
- Students working online from home are advised to use a table or desk, maintain good posture, and avoid extended use of mobile phones for learning tasks.

3.3 Digital Technologies for School Communication & Administration

- Google Workspace for Education (Gmail, Google Drive, Google Classroom) is the school's primary communication and collaboration platform.
- Vsware is the school's Information Management System (MIS), used for attendance, timetabling, class lists, assessment records, and school reports.
- Subject departments, committees, and working groups use Gmail and Google Drive for communication, meeting planning, and file sharing.
- Whole-school documents are stored and disseminated via email and/or Google Drive.
- Administrative staff use the school network for file storage and sharing.
- The school website and social media accounts are administered by KTCS and moderated by members of senior management and designated staff.
- Students who use laptops under the Assistive Technology Scheme

3.4 Digital Files for Submission to the State Examinations Commission (SEC)

- All video and/or audio recordings for SEC submissions must be made on networked school devices only.
- Specific network logins will be created for examination recording purposes.
- Recordings must be transferred and stored in accordance with DES/SEC instructions and removed from school devices as soon as possible thereafter.
- Personal devices must not be used for recording SEC examination material.

3.5 Junior Cycle Classroom Based Assessments (CBAs): Storage of Student Work

- Teachers must use school devices only for recording CBAs (desktop webcam or department device).
- CBA files must be uploaded to a designated Google Drive folder and stored only until the relevant Student Learning Achievement Report (SLAR) meeting is complete.
- Following the SLAR, CBA student data must be deleted from the school network and Google Drive.
- Subject departments may retain a small sample of anonymised student work for professional development purposes, stored in a secure, department-only Google Drive folder.
- Storage of student work or school data on personal devices outside the school network or Google Drive is a breach of GDPR and is strictly prohibited.

3.6 Artificial Intelligence (AI) Tools — New Section

3.6.1 General Principles

AI tools — including but not limited to ChatGPT, Google Gemini, Microsoft Copilot, and Canva AI — offer significant opportunities for learning, creativity, and productivity. However, their use must be governed by clear ethical principles to protect academic integrity, student wellbeing, and data privacy.

The following principles apply to all AI tool use in KTCS:

- AI tools are to be used only where explicitly permitted by a teacher or school policy.
- All users remain fully responsible for any content produced with the assistance of AI.
- AI-generated content must never be submitted as a student's own original work without clear teacher guidance and/or disclosure.
- No personal data — including student names, class groups, staff information, or school-sensitive material — may be entered into any publicly accessible AI tool.

- AI tools may not be used during formal school assessments or examinations unless explicitly permitted by the SEC or the classroom teacher.

3.6.2 Use of AI by Students

- Students may use AI tools for research support, idea generation, or editing assistance only with explicit teacher permission.
- Students must disclose AI use where directed to do so by their teacher.
- Submitting AI-generated content as one's own work in any assessment — including Junior Cycle CBAs, Leaving Certificate coursework, or class-based tasks — constitutes academic dishonesty and will be treated as a breach of the Code of Behaviour.
- Students must not use AI tools to generate harmful, offensive, discriminatory, or misleading content.
- Students must not use AI tools to impersonate, defame, or bully others.

3.6.3 Use of AI by Staff

- Staff may use AI tools to support lesson planning, resource creation, feedback generation, and administrative tasks, subject to the conditions in this section.
- Staff must not input any personal student data, class lists, sensitive school information, or confidential material into any AI tool.
- Staff are responsible for critically reviewing all AI-generated content before use in a professional or educational context.
- Staff must model responsible and transparent AI use to students.
- Staff should engage with available CPD on the use of AI in education, as offered by the school, the PDST, or the Department of Education.

3.6.4 Generative AI and Copyright

- AI-generated content may involve copyright-protected material. All users must be mindful of copyright obligations under the Copyright and Related Rights Act, 2000.
- Users must not use AI tools to reproduce, repackage, or distribute copyrighted material without appropriate attribution or permission.

4. Acceptable and Unacceptable Use of ICT

4.1 General Principles

- Information security is everybody's responsibility.
- The school's ICT systems are provided primarily for educational use.
- Limited and reasonable personal use of the school's email system and internet is permitted for staff, provided it does not interfere with professional duties, does not breach any element of this policy, and does not bring the school into disrepute.
- All use of school ICT systems is subject to monitoring in accordance with the school's legal obligations.

Acceptable use includes:

- Accessing and using approved educational websites, platforms, and resources.
- Using Google Workspace for Education for school-related communication, collaboration, and learning.
- Using school devices for curriculum delivery, learning, assessment, and administration.
- Communicating professionally with students, parents/guardians, and colleagues via school-approved channels.
- Accessing CPD materials, educational research, and professional resources.
- Using school-approved AI tools in line with Section 3.6 of this policy.

Unacceptable use includes, but is not limited to:

Category	Examples of Unacceptable Use
Illegal activity	Accessing, creating, or distributing illegal content; hacking; cybercrime offences under the Criminal Justice (Offences Relating to Information Systems) Act, 2017
Inappropriate content	Accessing or distributing pornographic, violent, extremist, racist, or otherwise harmful material
Harassment & bullying	Cyberbullying, trolling, threats, defamatory posts, or impersonation of any person
Data breaches	Sharing personal data in breach of GDPR; storing student data on personal devices
Copyright infringement	Illegal downloading, sharing, or reproducing copyrighted material
Misuse of school accounts	Using another person's login; sharing passwords; using school accounts for personal commercial gain

Misuse of AI tools	Submitting AI-generated work as one's own; entering personal/sensitive data into AI tools
Unauthorised recording	Recording staff, students, or school activities without explicit permission
Social media misuse	Posting content that identifies, embarrasses, or endangers students or staff; misrepresenting the school
Personal misuse	Excessive personal internet use during school hours that impairs professional responsibilities

4.2 Internet Use — Students

Students may use the internet to:

- Access educational content and resources as directed by their teacher.
- Use Google Workspace tools for learning, collaboration, and assessment tasks.
- Research topics related to their studies.

Students may not use the internet to:

- Access social media platforms (e.g. Instagram, TikTok, Snapchat, YouTube) during class time unless explicitly directed by a teacher for educational purposes.
- Access gaming, gambling, or streaming sites during school hours.
- Download software, applications, or files without teacher/staff permission.
- Access any content that is illegal, harmful, or inappropriate.
- Conduct any activity that could endanger themselves or others.

4.3 Internet Use — Staff

- Staff must use school ICT resources primarily for professional and educational purposes.
- Staff must model responsible digital citizenship for students.

- Staff must never access, download, or distribute illegal, inappropriate, or harmful content on school devices.
- Staff are required to read and sign the Staff AUP Agreement (Appendix B) annually.
- Staff using personal devices for school purposes must ensure those devices are adequately secured (password-protected, up-to-date antivirus software, encrypted where possible).
- Under no circumstances should personal devices be used to store student personal data.

4.4 Use of Mobile Phones & Personal Devices

In accordance with the Department of Education Circular 0027/2024 (or updated circular, as applicable), Kildare Town Community School operates the following mobile phone policy:

- Students are not permitted to use personal mobile phones or smart devices during the school day, including breaks and lunch.
- Mobile phones must be switched off and stored in school bags upon arrival at school and may only be retrieved at the school gate at the end of the school day.
- Phone pouches are present in classroom
- Exceptions may be made for students with specific medical or special educational needs, where agreed in advance with the Principal.
- Staff may use personal mobile phones for professional purposes during the school day but must exercise professional discretion, particularly when in the presence of students.
- Staff must not use personal mobile phones to photograph, record, or video students at any time.
- Breaches of the mobile phone policy by students will be addressed in accordance with the school's Code of Behaviour.

4.5 Email & Online Communication — All Users

- All school email communication must be conducted via the school's Google Workspace (Gmail) accounts.
- Staff must not use personal email accounts to communicate with students or parents/guardians.

- Email communications must be professional, respectful, and appropriate.
- Staff must not communicate with students via personal social media accounts or personal messaging apps (e.g. WhatsApp, Snapchat, Instagram DMs).
- Students must not use school email accounts for personal or inappropriate communications.
- Any threatening, abusive, or inappropriate emails received by staff or students must be reported to the Principal immediately.

4.6 Social Media

- The school's official social media accounts are managed by designated staff under the supervision of senior management.
- Staff must not post, share, or comment on social media in a manner that identifies, embarrasses, or could cause harm to students, parents/guardians, colleagues, or the school.
- Staff must not use social media to contact students unless via an official, school-sanctioned platform.
- Students must not post content online that defames, bullies, or endangers any member of the school community.
- Cyberbullying occurring outside of school — including via social media — that impacts the school community will be addressed in accordance with the school's Anti-Bullying Policy.

4.7 Photography, Video & Audio Recording

- The recording of students (video, audio, or photography) on school premises or at school events is subject to the school's GDPR/Data Protection Policy and requires explicit consent.
- Staff must never photograph or record students on personal devices without prior written consent from parents/guardians (for students under 18) or from the student (if 18+).
- Students must not photograph, video, or audio-record staff, other students, or school activities without explicit permission.
- Sharing images or recordings of students on social media or other public platforms without consent is a serious breach of this policy and may constitute a breach of GDPR.

5. Data Protection & GDPR Compliance

This section should be read in conjunction with the school's full GDPR/Data Protection Policy.

- All personal data collected and processed by KTCS is handled in compliance with the General Data Protection Regulation (GDPR), 2018 and the Data Protection Act, 2018.
- Student data — including names, dates of birth, attendance records, assessment results, and SENCO information — must only be accessed by authorised staff for legitimate school purposes.
- Personal data must not be shared with third parties without appropriate consent or a lawful basis for processing.
- All staff are required to complete GDPR awareness training as part of their induction and at regular intervals thereafter.
- Data breaches — including loss, unauthorised access, or accidental disclosure — must be reported to the school's Data Protection Officer (DPO) or designate immediately and no later than 72 hours after becoming aware of the breach, in line with GDPR obligations.

Key GDPR obligations for all staff:

- Access only the personal data you need for your role.
- Store personal data only on approved school systems (school network or Google Drive).
- Do not transfer personal data to personal devices or personal cloud accounts.
- Log out of all school systems when finished.
- Use strong, unique passwords and do not share login credentials.
- Report any suspected data breach immediately.

6. Cyberbullying & Online Safety

KTCS is committed to ensuring a safe online environment for all members of the school community in accordance with the Online Safety and Media Regulation Act, 2022 and the school's Anti-Bullying Policy.

- Cyberbullying — whether occurring on school systems or via personal devices, inside or outside of school — that impacts the school community will be investigated and addressed in accordance with the school's Anti-Bullying Policy.
- Students and staff who experience cyberbullying must report it immediately to their year head, class tutor, or the Principal/Deputy Principal.
- The school will co-operate fully with An Garda Síochána in any investigation of online harassment, abuse, or criminal activity involving members of the school community.
- Staff who receive threatening, abusive, or inappropriate electronic communications must report these immediately to the Principal.
- The school provides age-appropriate cyber-safety education to students through SPHE, CSPE, and relevant subject classes as part of the Wellbeing Programme.

7. Filtering, Monitoring & Network Security

7.1 Internet Filtering

- The school network uses content filtering software to restrict access to inappropriate, harmful, or illegal websites.
- Filtering is applied to all devices connected to the school network, including school-owned devices and personal devices using the school Wi-Fi.
- Filtering is not infallible. Students and staff who accidentally access inappropriate content must report it immediately to the teacher or a member of senior management.

- Attempting to bypass, disable, or circumvent the school's content filtering systems — including through the use of VPNs, proxy servers, or other methods — is a serious breach of this policy and will be sanctioned accordingly.

7.2 Network Monitoring

- The school reserves the right to monitor all use of its ICT infrastructure, including internet browsing history, email communications, file storage, and activity on the school network.
- Monitoring is conducted to ensure the safety of users, compliance with this policy, and adherence to the school's legal obligations.
- Users have no expectation of privacy in respect of their use of school ICT systems.
- Monitoring is carried out in accordance with the Interception of Postal Packets and Telecommunications Messages Act, 1993, GDPR, and the school's Data Protection Policy.

7.3 Network Security

- All users must use strong, unique passwords for their school accounts and must not share login credentials with any other person.
- Students must not attempt to access another student's or staff member's account.
- Staff must not share network passwords with students.
- Any suspected breach of network security — including unauthorised access or suspicious activity — must be reported to the ICT coordinator or Principal immediately.
- All school devices must be logged out of at the end of each session.
- USB/flash drives and external storage devices may only be used on school devices with the permission of the class teacher or ICT coordinator.

8. Roles & Responsibilities

8.1 Board of Management

- Ratifies and approves this policy and all associated policies.
- Ensures that adequate resources are allocated for ICT infrastructure, maintenance, and staff training.
- Reviews this policy at least every two years or following any significant legislative or operational change.
- Ensures the school fulfils its obligations under the Children First Act, 2015, GDPR, and the Online Safety and Media Regulation Act, 2022.

8.2 Principal & Deputy Principal

- Lead the implementation of this policy and all related school policies.
- Ensure all staff, students, and parents/guardians are informed of and have access to this policy.
- Ensure that all staff receive appropriate training on ICT, GDPR, and online safety.
- Investigate and respond to all reported breaches of this policy.
- Liaise with the DES, An Garda Síochána, Tusla, and other statutory agencies as required.
- Maintain oversight of the school's ICT infrastructure in collaboration with the ICT Coordinator.
- Ensure AI tool use in the school is reviewed and governed in line with updated DES guidance.

8.3 ICT Coordinator

- Manages the day-to-day operation of the school's ICT infrastructure, including the network, Google Workspace, and school devices.
- Oversees the implementation of content filtering and network security measures.
- Advises the Principal and Board of Management on ICT-related matters, including emerging technologies and policy updates.

- Manages access credentials for staff and students.
- Leads ICT-related CPD for staff, as appropriate.
- Reports ICT-related issues, including security incidents, to senior management.

8.4 Teaching Staff

- Read, understand, and comply with this policy in full.
- Sign the Staff AUP Agreement (Appendix B) annually.
- Supervise students' use of ICT at all times during class.
- Model responsible and ethical digital behaviour for students.
- Report any breaches of this policy by students or other users to senior management.
- Integrate digital citizenship and cyber-safety into teaching and learning, as appropriate to their subject area.
- Ensure that school devices and accounts are used in compliance with this policy and GDPR.
- Engage with CPD on ICT, online safety, GDPR, and AI as provided by the school or PDST.

8.5 Non-Teaching & Administrative Staff

- Read, understand, and comply with this policy in full.
- Sign the Staff AUP Agreement (Appendix B) annually.
- Use school ICT systems only for authorised school business.
- Handle all student and staff personal data in accordance with GDPR and the school's Data Protection Policy.
- Report any suspected data breaches or misuse of ICT systems to the Principal immediately.

8.6 Students

- Read and sign the Student AUP Agreement (Appendix C) at the beginning of each academic year.
- Use school ICT systems responsibly, ethically, and in compliance with this policy.
- Never attempt to access inappropriate, harmful, or illegal content.
- Never share login credentials with any other person.
- Never use school systems to bully, harass, or threaten any other person.
- Report any accidental access to inappropriate content or any instance of cyberbullying to a teacher or member of staff immediately.

- Comply with the school's mobile phone policy (Section 4.4) at all times.
- Use AI tools only where explicitly permitted and in accordance with Section 3.6 of this policy.

8.7 Parents & Guardians

- Read and sign the Parent/Guardian AUP Agreement (Appendix D) on enrolment and at the beginning of each academic year.
- Support the school in promoting responsible digital citizenship at home.
- Monitor their child's use of digital devices and internet access outside of school hours.
- Encourage their child to adhere to the school's mobile phone policy and this AUP.
- Report any concerns about cyberbullying, inappropriate online content, or online safety to the school immediately.
- Engage with online safety information and resources provided by the school, including webinars, information evenings, and Webwise resources.

9. Sanctions

Breaches of this Acceptable Use Policy will be addressed in accordance with the school's Code of Behaviour and relevant statutory law. The severity of the sanction applied will reflect the nature, seriousness, and context of the breach.

Category of Breach	Possible Sanction
Minor breach (e.g. accessing a non-educational site during class)	Verbal warning; temporary suspension of ICT privileges
Moderate breach (e.g. repeated misuse; inappropriate content access)	Written warning; meeting with year head/principal; suspension of ICT privileges
Serious breach (e.g. cyberbullying; GDPR breach; recording without consent)	Formal disciplinary process under Code of Behaviour; parental notification; possible suspension
Very serious/criminal breach (e.g. accessing illegal content; hacking; sharing CSAM)	Immediate referral to An Garda Síochána; Tusla notification where child protection concerns arise; possible expulsion

10. GDPR & Data Protection — Summary Obligations

This section summarises key obligations. The full KTCS Data Protection/GDPR Policy must be consulted for complete guidance.

All users must:

- Access only personal data necessary for their role.
- Store personal data only on school-approved systems (school network or Google Drive).
- Never transfer student or staff personal data to personal devices or personal cloud accounts.
- Log out of all school systems after each session.
- Use strong, unique passwords and never share login credentials.
- Report any suspected data breach to the Principal or designated Data Protection lead within 24 hours of becoming aware of it.

11. Policy Review & Monitoring

Item	Detail
Review Frequency	Every two years, or sooner if required by legislative change, DES guidance, or significant incident
Responsibility for Review	Principal, ICT Coordinator, and relevant staff
Approval	Board of Management
Monitoring	Ongoing — ICT Coordinator, Deputy Principal, and Principal
Staff Awareness	Policy shared with all staff annually; signed agreement required
Student Awareness	AUP introduced to all students at start of academic year; signed agreement required
Parent/Guardian Awareness	AUP shared via school website, Vsware, and annual notification

12. Related Policies

The following school policies must be read in conjunction with this AUP:

- Code of Behaviour
- Anti-Bullying Policy
- Child Safeguarding Statement
- GDPR / Data Protection Policy
- Social Media Policy
- Remote / Blended Learning Policy
- Mobile Phone Policy
- Attendance Policy
- Wellbeing Policy

All policies are available on the school website.

13. References & Guidance Materials

- Department of Education — *Digital Strategy for Schools to 2027*
- Department of Education Circular 0027/2024 — Mobile Phones in Schools
- Webwise — www.webwise.ie
- National Council for Curriculum and Assessment (NCCA) — Junior Cycle & Leaving Certificate specifications
- Data Protection Commission (DPC) — www.dataprotection.ie
- Tusla — www.tusla.ie
- An Garda Síochána — Cyber Crime Bureau
- Children First National Guidance, 2017
- Online Safety and Media Regulation Act, 2022



15/06/2026