De La Salle College, Dundalk
Acceptable Usage Policy (AUP)

1. Purpose & Scope

The Acceptable Usage Policy (AUP) sets out the standards and expectations for the safe, ethical and responsible use of ICT in De La Salle College, Dundalk. It applies to all students, teachers, staff, parents/guardians, contractors and visitors who use or access school ICT systems, internet, networks, devices, email, cloud services, and remote learning platforms.

The purpose is to:

- Protect students and staff from risks associated with digital technologies.
- Promote digital literacy, respect, and responsible online citizenship.
- Ensure compliance with Irish legislation, GDPR, and Department of Education policies.
- Safeguard the school's reputation and maintain a safe learning environment.

2. Relevant Legislation & Policy Context

This AUP is informed by the following legislation and policies:

- General Data Protection Regulation (GDPR) (EU 2016/679) and Data Protection Act 2018.
- Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law).
- Online Safety and Media Regulation Act 2022.
- Children First Act 2015 and Child Protection Procedures for Primary and Post-Primary Schools (2017, updated 2025).
- Anti-Bullying Procedures for Primary and Post-Primary Schools (2013).
- Department of Education Circular 0045/2025 on Mobile Phone Use in Post-Primary Schools.
- Teaching Council Code of Professional Conduct (2021).
- SEC guidance on Artificial Intelligence in Coursework (2024/2025).

3. Roles & Responsibilities

- Students: Act responsibly online, follow rules, report concerns, protect personal data and passwords.
- Staff: Model positive ICT use, uphold safeguarding standards, use professional communication.
- Parents/Guardians: Support the school's digital learning, discuss safe ICT use at home, monitor devices.
- ICT Coordinator: Maintain filtering, monitoring, training, technical support.
- Designated Liaison Person (DLP): Manage ICT-related safeguarding incidents.
- Board of Management: Ratify and review this AUP annually.

4. Filtering, Monitoring & Privacy

The school uses the PDST/HEAnet broadband service with filtering set at Level 4, which allows access to educational YouTube content under teacher supervision while blocking social networking and inappropriate sites.

Monitoring: All internet, email and device use is logged for safeguarding, child protection, security, and network management. Monitoring is proportionate and in compliance with GDPR. Logs are stored securely, accessed only by authorised staff, and retained for the minimum necessary period.

5. Mobile Phones

In line with Department of Education Circular 0045/2025, students are not permitted to use personal mobile phones during the school day. This includes calls, messages, social media, and photography. Exceptions may be granted for medical or additional learning needs with prior approval. Confiscation and disciplinary measures will apply to breaches of this policy.

6. Email, Messaging & Collaboration Tools

Each student is assigned a school-managed email account and Microsoft Teams/Google Workspace login. These are to be used exclusively for school-related work. Students must:

- Communicate respectfully at all times.
- Not use anonymous or false accounts.
- Not send or share offensive, illegal, or bullying messages.
- Use chat functions appropriately for educational purposes only.

All communications may be monitored.

7. Images, Audio, Video & Recording

The use of images, audio, and video must comply with GDPR and safeguarding requirements:

- Consent is required for use of student images in publications, websites, or social media.
- Parents/guardians may select consent options on a granular basis (website, apps, social media, press).
- Students and staff may not record lessons, meetings, or conversations without prior approval.
- SEN/assistive technology exceptions may be authorised for learning support.
- Approved recordings must be stored securely, used for the stated purpose only, and deleted afterwards.

8. Artificial Intelligence (AI)

The school recognises the benefits and risks of generative AI tools (ChatGPT, image/video generators, coding assistants, etc.):

- Students must not present AI-generated work as their own.
- Any use of AI must be acknowledged and referenced.
- SEC guidelines (2024/25) confirm that AI-generated material receives no credit in coursework; only the student's original work will be assessed.
- Teachers may use AI for lesson planning or resource creation with discretion, while ensuring professional judgment and data protection compliance.
- AI detectors are not relied upon as sole evidence of misuse.

9. Cyberbullying & Harmful Communications

The school has a zero-tolerance approach to bullying, online harassment, and harmful communications. Under Coco's Law (2020), it is a criminal offence to share intimate images without consent or to cause harm online. Any such incidents will be dealt with under the Anti-Bullying Policy, Code of Behaviour, and where necessary referred to An Garda Síochána.

10. Personal & School Devices (BYOD/1:1)

The school operates a 1:1 device programme for Senior Cycle students. Requirements include:

- School devices are enrolled in Mobile Device Management (MDM) with approved software/apps only.
- Students must keep devices charged and maintained.
- Loss or damage must be reported immediately.
- BYOD devices (where approved) must meet security requirements: antivirus, updates, secure passwords.
- Device use during exams is strictly prohibited unless approved for accommodations.
- Devices remain the property of families but must be surrendered for inspection if policy breaches are suspected.

11. Remote & Online Learning

During remote or hybrid learning:

- Students must use real names and log in with school accounts.
- Cameras should be used in appropriate environments with neutral backgrounds.
- Private chat is not permitted unless directed by the teacher.
- Staff may not conduct unscheduled 1:1 video calls with students.
- Any recordings must be pre-approved, stored securely, and deleted after use.

12. Copyright & Licensing

All students and staff must respect copyright law:

- Only approved or licensed resources may be used.
- Free/open-source material may be used if properly credited.
- Copying, pirating, or illegally downloading software/media is prohibited.
- AI-generated material must be acknowledged as per SEC guidelines.

13. Incident Response

In the event of a breach:

- Students must report issues to a teacher immediately.
- Staff must escalate incidents to the ICT Coordinator, Principal or DLP.
- Illegal content, image-based abuse, or online harassment will be reported to An Garda Síochána.
- Data protection breaches will be reported to the Data Protection Commission as required.
- Sanctions may include warnings, loss of ICT privileges, suspension, or expulsion (in line with the Code of Behaviour).

14. Review & Ratification

This policy will be reviewed annually by the Board of Management. It was adopted on [date] and is subject to regular updates in line with new legislation, Department circulars, and emerging technologies.

Appendix A – Student & Parent Consent Form

I have read and understood the Acceptable Usage Policy. I agree to abide by the rules outlined.

Consent Options (please tick):
[ ] Use of student image in school website/publications
[ ] Use in school social media platforms
[ ] Use in local/national press
[ ] No consent given

Student Name: ____________________ Class: ________
Parent/Guardian Signature: _________________________ Date: ______
Student Signature: ______________________________ Date: ______