

# St. Mary's College Dundalk



## Acceptable Use Policy.

*Ratified by the Board of Management on 22<sup>nd</sup> June 2026.*

## **St Mary's College Mission Statement.**

St Mary's College is a Catholic secondary school under the patronage of the Marist Fathers. The primary aim of the College through its spiritual and humanistic endeavours, is to promote and develop a sense of community where those entrusted to its care can be brought to the fullness of their human potential in accordance with the teachings of the Gospel.

The College, through its academic, pastoral and spiritual undertakings strives to provide for the holistic development and welfare of each of the students in its care.

## **Aims of AUP.**

1. This Acceptable Use Policy (AUP) aims to ensure the students of St Mary's College benefit from the learning opportunities our technology and digital resources provide, in a safe and responsible manner.
2. To ensure the ethical use of technology while in the College, students must use chrome books, desktop computers, laptops, computer networks, social media (where use is approved) and all forms of Internet access solely for the purpose and promotion of curriculum / College-based education.
3. Access to digital resources and internet is considered a privilege. Therefore, where this policy is not adhered to, this privilege may be withdrawn and where necessary, sanctions imposed.
4. The College recognises the rapidly evolving nature of digital technologies, including Artificial Intelligence (AI), cloud-based systems, wearable technology, messaging platforms and emerging social media applications. This policy aims to promote digital wellbeing, online respect, cyber safety, data privacy and responsible digital citizenship for all members of the College community.
5. The College is committed to supporting students in developing the skills required to critically evaluate online information, misinformation, manipulated content and AI-generated material.

St Mary's College and relevant stakeholders will revise this Acceptable Use Policy at regular intervals. Before signing, the policy should be read carefully by students and Parents / Guardians to ensure that the conditions of use are accepted and understood.

## **College Strategy.**

1. Students and teachers will be provided with guidelines in the area of Internet safety.
2. The College engages an external specialist service to support the monitoring, protection, and ongoing improvement of the school's network safety.
3. The use of IT in classes will be under the supervision of a teacher.
4. Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
5. The College will regularly monitor students' Internet usage.
6. Virus protection software will be used and updated on a regular basis.
7. Multi-factor authentication, secure passwords and account protection measures may be implemented where appropriate to enhance cybersecurity.

8. Students must not share passwords, login credentials or authentication codes with others.
9. The College reserves the right to temporarily restrict access to online systems or accounts where there is a concern regarding safeguarding, cybersecurity or misuse.
10. Recording, livestreaming or screen capturing of lessons, meetings or College activities without explicit permission is prohibited.

#### **Online & Artificial Intelligence (AI).**

- Students will not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Students will never disclose or publicise personal information.
- Students taking steps to bypass content filtering by using proxy sites, VPNs, anonymising tools or other means is prohibited.
- Should students use Artificial Intelligence tools, they will acknowledge this within their work.
- AI tools must not be used to cheat / deceive, impersonate, create fake communications, generate harmful material or bypass normal assessment procedures.
- Students must not engage in cyberbullying, anonymous messaging, misrepresentation, image-based abuse ('deepfakes') or the sharing of harmful digital content.
- Students must not use personal or College devices to access, generate or distribute explicit, violent, discriminatory or extremist material.
- Students must immediately report any suspected hacking, phishing attempts, scams, inappropriate contact or safeguarding concerns to a member of staff.
- Students are prohibited from using another person's account, profile or identity online.
- The publication or sharing of data, photographs, videos or recordings of any stakeholder of the college community, without consent, is prohibited. Students should maintain respectful communication in all digital interactions associated with the College, whether inside or outside of school hours.

#### **Social Media Accounts.**

- Students are not permitted to use social media apps within the College campus or post in relation to school activities, without explicit permission from Senior Management / Staff Member.
- Chat rooms, discussion forums and online communication forums will only be used for educational purposes.
- Profile pictures and avatars, where used, must be appropriate and respectful.
- Anonymous accounts, parody accounts or impersonation accounts relating to any stakeholder of the College, are prohibited.
- Students must not participate in online trends, challenges or content creation that may place themselves or others at risk. Any online behaviour that negatively impacts the wellbeing, dignity or reputation of members of the College community or the College itself, may be investigated under the Code of Behaviour.

### **College Website.**

The website will be regularly checked to ensure that there is no content that compromises the safety of students or staff.

The College will endeavour to use digital photographs, audio or video clips focusing on group activities.

Students are not permitted to post information to the College website. College activities are managed online by our Public Relations Coordinator.

### **Data Protection and Safeguarding**

The College is committed to protecting the privacy, dignity and personal data of all members of the College community.

Personal data will be processed in line with GDPR, the Data Protection Act 2018 and Department of Education guidance.

Digital safeguarding concerns may be managed in accordance with the College's Child Protection procedures.

### **Legislation**

- EU General Data Protection Regulation (GDPR) 2016/679.
- Data Protection Act 2018.
- Children First Act 2015.
- Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law).
- Criminal Justice (Offences Relating to Information Systems) Act 2017.
- Copyright and Related Rights Act 2000 (as amended).
- Online Safety and Media Regulation Act 2022.
- Digital Services Act (EU) 2022.
- Guidance issued by the Department of Education and Oide Technology in Education relating to AI and digital technologies.

### **College Policies linked to AUP**

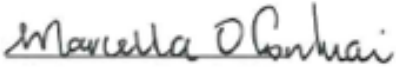
- Code of Behaviour.
- Child Protection.
- Teaching and Learning Policy.
- Homework and Study Policy.
- AEN Policy.
- Bí Cinealta Policy.
- Data Protection Policy.
- Critical Incident Policy.

### Sanctions

- Breaches of this policy may result in disciplinary action, including warning, detention, withdrawal of access privileges, suspension and / or expulsion, as per the College's Code of Behaviour.
- The College reserves the right to report illegal activities to the appropriate authorities.

### Evaluation of AUP

- This Policy will be reviewed as deemed necessary.

Signed: 

Date: 22<sup>nd</sup> June 2026

Mrs. Marcella Ó Conluain,  
Chairperson of Board of Management.

## **Appendix.**

### **Addendum: One-to-One Digital Student Devices**

From December 2026, 5th year students will participate in a 1:1 device programme.

#### **Rationale**

The use of individual laptops in this environment offers significant opportunities to enhance each student's overall learning experience. At St Mary's College, these devices provide students with the flexibility to learn anytime and anywhere, both in the classroom and at home. A 1:1 personalised learning approach helps to reduce the digital divide and encourages responsible engagement with rapidly evolving technologies.

The purpose of this programme is to ensure that all students can benefit fully from digital teaching and learning opportunities. St Mary's College is committed to creating a safe, secure, and supportive learning environment that fosters mutual respect and responsibility across the College community.

The integration of mobile learning into classrooms supports the development of essential 21<sup>st</sup> century skills, preparing students for further education as well as their future social and professional lives.

The programme is closely aligned with the College's Code of Behaviour, Acceptable Use Policy, Bí Cineálta Policy and Data Protection Policy (please note – this list of policies is not exhaustive).

#### **General Rules – Care, Use & Precautions.**

Students are expected to use their devices responsibly, safely, and in line with College expectations at all times.

- Students are responsible for the general care and condition of their device.
- Any device that is damaged or not functioning properly must be reported immediately and brought to a Deputy Principal for evaluation.
- Devices are to be used only for educational purposes, including classwork and homework.
- Devices must remain in their protective case when not in use, both in school and at home.
- Students must arrive to school each day with their device adequately charged (minimum 80%). Charging devices in the College is not permitted.
- Devices must remain in school bags when not in use and only placed on desks when instructed by a teacher.
- When not required during class, devices must be fully closed and placed flat on the desk.
- Devices must never be left unsupervised, e.g., in an unlocked locker.
- Care must be taken with cables; they should be handled and stored correctly to avoid damage.
- Devices must not be stored in the same compartment as water bottles. Water bottles are not permitted on desks during class.

- Screens must be cleaned using a soft, dry cloth only.

#### Screen Care.

- Device screens are sensitive and can be easily damaged by pressure.
- Students should not lean on devices when closed.
- Objects should not be placed on or near devices where pressure could be applied.

#### Use, Restrictions and Sanctions.

- Students must use devices in accordance with this policy, the Code of Behaviour, and any other relevant policy.
- Misuse of devices may result in restricted access, temporary confiscation, or loss of device privileges.

#### Examples of Misuse – please note this list is not exhaustive.

- Unauthorised audio/video recording, use of camera or inappropriate use of apps.
- Accessing inappropriate, offensive, defamatory or illegal content.
- Cyberbullying, harassment or disrespectful conduct.
- Using another student's device or accessing their accounts / data.
- Attempting to hack or bypass College systems.
- Installing or distributing copyrighted material illegally.
- Gaming or using devices for non-educational purposes during class.
- Vandalism or intentional damage to hardware, software or data.
- Use of chat rooms or unauthorised communication platforms.
- Failure to cooperate with college investigations.
- Repeated failure to bring a device or failure to bring it in sufficiently charged.

#### Restricted Use and Confiscation.

- Students may be placed on restricted or limited device use at the discretion of the Senior Management of the College.
- Devices may be confiscated for a limited period where misuse occurs; if misuse continues, a permanent ban may be applied.
- Device privileges will only be restored when Senior Management / the Board of Management is satisfied that expectations have been met.

### **Substitution of Equipment.**

- Where a student's device is inoperable, the College may provide a substitute device (subject to availability).
- Students are responsible for the care and proper use of any substitute device.
- Damage to a substitute device is the responsibility of the student and their parent / guardian.
- Only one substitute device will be issued at any one time.
- Where a substitute device is misused, not brought in to school or not charged a replacement will not be issued.
- Where no substitute is available, students must use hard copy materials.
- Devices may not be borrowed without permission.

### **Roles & Responsibilities of College Stakeholders.**

#### **Student Responsibilities**

Students must:

- Arrive to school each day with an adequately charged device (minimum 80%).
- Use all devices in a responsible, ethical and appropriate manner.
- Follow teacher instructions regarding device use.
- Report any issues, damage or malfunction immediately.
- Power down devices when finished.
- Report any inappropriate or abusive content encountered.
- Ensure all work submitted is their own:
  - ✓ Plagiarism is strictly prohibited.
  - ✓ Translation tools must not be used for assessed work unless permitted.
  - ✓ AI tools must not be used to complete assigned work unless explicit permission is given by teacher.
- Respect copyright and intellectual property rights.
- Not allow others, with the exception of parents / guardians, to use their device.
- Not use another student's device under any circumstances.

## **Parent / Guardian Responsibilities**

### **Equipment and Ownership**

- Parents/Guardians are responsible for:
  - ✓ Purchasing the device and required eBooks / apps.
  - ✓ Insurance, maintenance, repair and safe keeping of the device.
- While ownership remains with the parent / guardian, however, the College reserves the right to:
  - ✓ Collect, inspect or temporarily confiscate a device.
  - ✓ Alter, install or remove software where necessary.

## **Parent / Guardian Oversight**

### **Parents/Guardians must:**

- Ensure timely ordering / payment of the device.
- Discuss appropriate online behaviour and digital responsibility.
- Sign all required Acceptable Usage and Data Protection documentation.
- Regularly inspect the device and ensure it is in good working order.
- Regularly check installed apps and internet usage / history.
- Monitor device for inappropriate use or content.
- Report immediately to a member of Senior Management, any:
  - ✓ Damage.
  - ✓ Misuse.
  - ✓ Issues relating to ownership, possession or use.

## **Damage or Loss of Equipment**

- Damage or loss due to negligence or misuse is the financial responsibility of parents / guardians.
- The College will assist in liaising with Wriggle where appropriate.
- Please note - all devices are covered by a manufacturer's warranty for defects, subject to terms and conditions.

## **College Responsibilities**

### **The college will:**

- Provide filtered internet access and student email accounts.
- Take reasonable steps to block inappropriate online content.

- Provide guidance on:
  - ✓ Responsible digital behaviour.
  - ✓ Online safety.
  - ✓ Academic integrity and research practices.
- Support staff and students in implementing this policy.
- Report incidents of damage and/or misuse to parent / guardian.

**Please note:**

Devices remain the property of parent / guardian, and as such, the College is not responsible for their loss, theft or damage.

Wriggle devices are under a three-year warranty; however, parents / guardians may choose to privately take out specific insurance cover for their device.