Acceptable Use, ICT and Mobile Device Policy

1. Introduction

Our Lady of Mercy College school is committed to fostering a respectful, inclusive, and supportive learning environment that reflects the values of the Mercy Ethos and supports the holistic development of each student. Information and Communication Technology (ICT) resources are provided to support students' educational and personal growth, equipping them with digital skills necessary for the future.

This Acceptable Use Policy (AUP) outlines the rules, responsibilities, and expectations for the use of Information and Communication Technology (ICT) and digital resources in the school.

The AUP ensures that ICT is used in a safe, responsible, respectful, and educationally purposeful way, while protecting the wellbeing of students and staff.

This Acceptable Use Policy (AUP) policy aligns with our Mission Statement, which emphasises **"respect for all and the nurturing of individual potential, academically, spiritually, and culturally as a member of the school community."** ICT use should reflect these values by promoting learning, cooperation, kindness, and a safe digital environment.

Cyber Safety and Digital Literacy

As part of our commitment to student welfare, the school will provide guidance on cyber safety and responsible digital citizenship. Through structured lessons and workshops, students will learn about privacy, digital footprint management, and safe online practices.

Please note The use of the word parent refers to parent and or guardian

2. Policy Framework

2.1 This AUP is informed by:

- Department of Education **Circular 0045/2025** restricting personal mobile phone use in schools.
- **Bí Cineálta Procedures (2024)** to prevent and address bullying behaviour, including cyberbullying.
- The **Digital Strategy for Schools to 2027** and the Wellbeing Policy Statement (2019).
- Relevant legislation including: Data Protection Acts 1988–2018 and GDPR, Coco's Law 2020, Children First Act 2015, Copyright and Related Rights Act 2000.
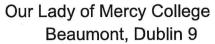
3. Scope

3.1 This policy applies to:

- All students, staff, and visitors who access school ICT systems or digital resources.
- All use of ICT within the school, during school activities, or when representing the school.
- All school-owned devices, accounts, and digital learning platforms.

It covers:

- Internet and network use
- Email and communication platforms
- Digital learning environments
- Artificial Intelligence (AI) tools
- Mobile phone and personal device use

4. No Personal Device School

In line with Circular 0045/2025, Our Lady of Mercy College is a **No Personal Device School**.

Students are not permitted to use personal mobile phones, smart watches, or internet-enabled devices during the school day.

Phones should be left at home. Or locked in the pouches provided. If brought to school, they must be powered off and stored in a designated school-approved pouch.

Exemptions may apply for medical or additional educational needs (e.g. diabetes monitoring, educational use under guidance of a teacher). Such exemptions must be formally approved by school management.

If a student forgets their phone they must give their phone into the school office for the duration of the school day.

Breaches will be addressed under the **Code of Behaviour**. If a student is found to be misusing a phone their phone will be confiscated and given to the Deputy Principal until the end of the school day. The issue will subsequently be addressed under the Code of Behaviour.

Risk to expensive personal electronic equipment The college authorities cannot be responsible for the safe keeping of various items of electronic equipment that students choose to bring to school. These items are brought onto the school premises at the students' own risk.

5. General ICT Use

Students are expected to:

- Use ICT **for educational purposes only**.
- Treat all ICT equipment with respect.
- Keep passwords and login details secure.
- Follow teacher directions when using ICT in class.

Students must not:

- Access or share illegal, obscene, hateful, or harmful content.
- Download unauthorised software or apps add files to device or USB.
- Circumvent security, filtering, or monitoring systems.
- Engage in behaviour that brings the school into disrepute.

- The charging of phones or other electronic equipment is not permitted unless permission is given from the class teacher.

6. Internet and Online Safety

Students will:

- Use the Internet for **educational purposes only**.
- Report accidental access to inappropriate material.
- Credit all sources and avoid plagiarism.

Students must not:

- Intentionally visit inappropriate sites.
- Reveal personal details or those of others online.
- Arrange meetings with strangers contacted online.

- Use AI to complete school assignments.

7. Email and Digital Platforms

Students will:

- Use only school-provided email accounts and platforms.
- Communicate respectfully, showing kindness in line with **Bí Cineálta**.

- Log out of all accounts and report accounts left logged in.

Students must not:

- Send or forward offensive, threatening, or discriminatory messages.
- Use school emails for personal social media, gaming, or online shopping.
- Share login details or access another person's account.

8. Social Media and Messaging

Students and staff must not use social media or messaging platforms to:

- Harass, impersonate, or insult others.
- Share school-related images, recordings, or data without permission.
- Discuss confidential school matters.

Students must not create, post, or share material that brings the school into disrepute.

9. Images, Audio and Video

Students must not record, photograph, or video staff or other students without express teacher permission.

Parental consent will be sought before student work, photos, or recordings are published on the school website or other platforms.

Sharing explicit images/videos of minors is strictly prohibited and will result in serious disciplinary and legal consequences with the Gardai and legal representatives.

10. Cyberbullying and Misuse Online

Definition
Cyberbullying is strictly prohibited and includes the use of technology (social media, messaging services, gaming platforms, email, or other online communication) to intimidate, exclude, humiliate, or cause harm.

Unacceptable Behaviour
- Engaging in online activities with the intention to harm, harass, or embarrass another student, staff member, or member of the school community is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions.
- Examples include, but are not limited to:
  - Hurtful, abusive, or threatening messages (text, email, social media posts, private messages).
  - Malicious sharing of images, videos, or audio recordings without consent.

- o Setting up fake profiles or impersonating others online.
- o Deliberate exclusion from online groups or platforms.
- o Posting or forwarding rumours, gossip, or derogatory material about another person.

Scope

- The school recognises that cyberbullying may occur **inside or outside school hours** and **on or off school premises**.
- Where incidents involve members of the school community (students or staff) and impact on relationships, wellbeing, or the learning environment, the school reserves the right to **investigate and address such incidents** under the Code of Behaviour, the Anti-Bullying Policy, and this AUP.

Distinction between Bullying and Isolated Incidents

- Measures are taken within the school to ensure that staff and students understand that bullying is defined as *unwanted negative behaviour – verbal, psychological, or physical – conducted by an individual or group against another person (or persons) and which is repeated over time.*
- This definition includes **cyberbullying**, even when it happens outside the school or at night. A one off instance of negative behaviour towards another student is not bullying behaviour.However, a single hurtful message posted on social media can be considered bullying behaviour as it may be visible to a wide audience and has a high likelihood of being shared multiple times and so becomes a repeated behaviour.

School Response

- The school adopts the **Bí Cineálta Procedures** approach of *prevention, support, and restoration of relationships.*
- Preventative measures include digital citizenship education, awareness workshops, and promoting kindness and empathy online.
- Alleged incidents will be investigated promptly, fairly, and sensitively.
- Parents/guardians will be informed where appropriate, and students will be supported throughout the process.
- Serious cases may be reported to **Tusla** (Child and Family Agency) or **An Garda Síochána**, in line with the **Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law)**.

Sanctions

- Any student found to be engaging in cyberbullying or misuse of online platforms will face sanctions under the Code of Behaviour.
- Sanctions may include restriction of ICT privileges, parental notification, suspension, or expulsion in extreme cases.
- Illegal behaviour will be referred to the relevant statutory authorities.

11. Artificial Intelligence (AI)

Use of Artificial Intelligence (AI) in Schoolwork

Our school recognizes the value of technology, including artificial intelligence, in enhancing learning. However, in order to maintain academic integrity and foster independent learning, students are not permitted to use AI tools to complete written assignments, state exam coursework, or any other assessed work intended to reflect their own skills, knowledge, and understanding.

- **Prohibited Uses of AI**
  Students are prohibited from using AI applications to generate, edit, or otherwise complete assignments, homework, essays, or projects that contribute to graded coursework, particularly in state examination subjects e.g. image creation.
- **Permitted Uses of AI**
  AI may be used for learning purposes when explicitly allowed by a teacher for activities such as exploring ideas, practicing skills, or as a supplemental resource. However, any work submitted for evaluation must be the student's original work, without reliance on AI-generated content.
- **Academic Integrity and AI**
  Any use of AI to produce or alter assignments intended to assess the student's knowledge or skill level is considered academic misconduct and will be addressed accordingly. Students who submit AI-generated work as their own may face disciplinary actions and a review of their coursework by the appropriate school and examination authorities.

12. Monitoring and Privacy

The school reserves the right to monitor ICT use for compliance, safety, and network security.

Monitoring may include inspection of email, browsing history, and digital files.

All monitoring will be proportionate and compliant with GDPR.

13. Sanctions

Breaches of this policy may result in:

- Verbal or written warnings.
- Withdrawal of ICT privileges.
- Confiscation of personal devices.
- Parental contact.
- Suspension or expulsion for serious/repeated breaches.

Illegal activities will be reported to the relevant authorities.

14. Support Structures

14.1 Students and parents will be informed of support organisations dealing with online safety, including **Webwise**, **Tusla**, and the **Online Safety Commissioner**.

15. The School App

Purpose
The school app is the primary platform for communication with the school community. It is used to:
- Share news and celebrate student achievements.
- Provide parents and students with up-to-date school information.
- Enable parents to complete absence forms, late slips, and other required notifications.
- Facilitate communication between parents and the school.
- Process payments for school-related activities.

Parental Responsibility
- Parents/guardians are expected to **check the app regularly** to stay informed of school updates.
- Absence and late notifications must be submitted promptly via the app.
- All payments for activities and trips must be processed through the app, unless otherwise advised by the school.

Standards of Communication

- All communication conducted through the school app must be respectful, constructive, and in keeping with the school's ethos.
- The app should not be used to send urgent or sensitive messages. Such matters must be addressed by:
    - Contacting the school office by telephone.
    - Requesting a meeting with the relevant staff member through the school secretary.
    - Emailing the appropriate staff member directly via their school email address.

School Responsibility

- The school will ensure the app is regularly updated with relevant and accurate information.
- The app will be used to enhance home–school communication in a manner that is transparent, timely, and supportive of student learning and wellbeing.

16. Staff Guidelines

Use of Phones and Personal Devices

- Organisation of school events should be done using the **school landline** where possible.
- Staff should keep personal calls and texts to **break times**; phones must remain on **silent during class time**.
- If a teacher uses their personal device for school purposes during class (e.g., attendance, posting resources), they should **inform students of the purpose** of that usage.
- Where staff photograph or record for school purposes on a personal device, materials must be **transferred to school systems and deleted** from the personal device as soon as practical.

Data Protection Responsibilities

Staff are personally responsible for safeguarding all student data in line with **GDPR (2018) and the Data Protection Acts**.

Things to do:

- Log out from any workstation when finished (CTRL+ALT+DEL).
- Use **password-protected platforms** such as VSware for accessing student information.
- Use codes/abbreviations rather than full names when distributing information internally.
- Print selectively and double-sided; collect documents promptly from printers and keep print areas tidy.

Things not to do:

- Do not view sensitive school information in public places where it may be seen by others.

- Do not share school devices or home computers containing student data with family or friends.
- Do not include student names in email subject lines.
- Do not disclose or share confidential information without the **express authorisation of the Principal**.
- Do not leave confidential documents unattended at printers or photocopiers.

Printing

- Printers are for **educational use only**.
- Avoid unnecessary or repeat printing; check queues and printer status before resending jobs.
- Use photocopiers for large batch copying.
- Be mindful of the school's environmental impact.
- Never send students to collect any photocopying or printing.

Disciplinary Action

- Breach of this policy may result in disciplinary procedures as set out by the **Teaching Council** and the **Department of Education**.

Staff Acceptance

All staff must confirm their compliance with this policy by signing the **Staff ICT Acceptable Use Agreement** at the end of this document.

16. Review and Ratification

This AUP will be reviewed annually by the Digital Learning Team and Senior Leadership.

The policy was adopted by the Board of Management on: _____

17. Agreement Form

Students and parents sign this form using our school App

Student

I agree to follow the school's Acceptable Use Policy on ICT. I will use the internet and digital technologies responsibly and respectfully.

Student Name: _____

Signature: _____

Date: _____

Parent/Guardian

I have read the Acceptable Use Policy and discussed it with my child. I support the school's implementation of this policy.

Parent/Guardian Name: _____

Signature: _____

Date: _____

Ratified by the Board of Management on 10th September 2025

Signed:

Gerry Lambe Chairperson of BOM

Gerry Lambe 10/9/25