



Acceptable Use Policy

Our Lady of Mercy Secondary School 2023-2024

Policy Content:

1. Introduction & Rationale
2. Legislation & School Policy
3. Acceptable Internet Usage
4. Email
5. Social media Digital Citizenship
6. Personal Devices
7. School Website
8. Support & Further Information
9. Reporting on Inappropriate Content.
10. Misuse of Digital Technologies & Sanctions.

Introduction & Rationale:

This policy addresses all rights, privileges & responsibilities associated with the school use of Internet and Digital Technologies. It is informed by our school mission statement.

As we move forward with new educational changes namely in Junior Cycle practice, the Digital Learning Framework, the introduction of Computer Science at Senior Cycle the possibility of distance and blended learning due to COVID19 or other unforeseen restrictions, we move towards embedding digital technologies to create meaningful student learning experiences. By encouraging positive student engagement, we hope to realise and maximise the potential of digital technologies as a valuable resource for assessment and e-learning purposes in a safe and effective manner to enhance teaching and learning.

Legislation & School Policy that Govern and Guide Schools AUP:

1. The Harassment, Harmful Communications and Related Offences Act, 2020: This act makes it a criminal offence to distribute, publish or threaten to publish or distribute an intimate image of another person without their consent.
2. The Interception of Postal Packets and Telecommunications Messages Regulation Act, 1993: This Act stipulates that telecommunication messages can be intercepted for the purpose of an investigation of a serious offence.
3. The Video Recordings Act, 1989: This prohibits the distribution of videos, which contain obscene or indecent material, which may lead to the depravation, or corruption of the viewer.
4. The Child Trafficking and Pornography Act, 1998: This Act legislates against anyone who knowingly produces, prints, publishes, distributes, exports, imports, shows, possesses or sells child pornography.
5. The General Data Protection Regulation (GDPR) 2018: This Act was passed to deal with data processing, privacy issues arising from the increasing amount of Information kept on computer about individuals.

6. The Non-fatal Offences against the Person Act 1997: Section 10 (1) of this Act prohibits any person who, without lawful authority or reasonable excuse, by any means including by use of the telephone, harasses another by persistently following, watching, pestering, besetting or communicating with him or her, shall be guilty of an offence.
7. Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012: The Act creates a criminal offence of withholding information relating to the commission of a serious offence, including a sexual offence, against a person under 18 years or a vulnerable person.

School Policies that link to Acceptable Use Policy:

1. Child Safeguarding Statement (including Risk Assessment):
2. Health & Safety Policy Statement
3. Anti- Bullying Policy
4. Distance Learning Policy
5. Dignity at Work Policy
6. Code of Behaviour:
 - This outlines all school rules and sanctions in the event of breaches to school rules. Students are expected to follow the same rules for good behaviour and respectful conduct online as offline.
 - Misuse of school resources may result in disciplinary action. We make a reasonable effort to ensure students' safety and security online but will not be held accountable for any harm or damages that result from misuse of school technologies.
 - Students are expected to alert his/her teacher immediately of any concerns for safety or security.

Acceptable Internet Use Policy:

1. Internet Use:

- Students can only use the Internet when supervised by a teacher.
- Students will use the Internet for educational purposes only.
- Online shopping is prohibited.
- Access to instant messaging services is forbidden.
- Blogging can only be used under teacher supervision.
- Students cannot use Online Gaming Apps, unless under teacher permission & supervision.
- Students cannot use school computer equipment for commercial gain.

2. Inappropriate Content:

No user shall visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that relate to the promotion of: illegal acts, racist materials, pornography, child sexual abuse images, promotion of any kind of discrimination, threatening behaviour, including the promotion of physical violence or mental harm, or any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school.

3. E-Safety Education:

Students will be provided with information in the area of Internet safety.

4. National Centre for Technology in Education:

OLM's computer network is intended for educational purposes only. All activity over the network may be monitored and retained. Access to online content via the network is restricted in accordance with this AUP, our policies and the Department of Education and Skills through its agency, the National Centre for Technology in Education.

5. Web Filter:

Students are expected to respect that the web filter is a safety precaution and should not try to circumvent it when browsing the Web. Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material. If a site is blocked and a student believes it shouldn't be, the student can ask his/her teacher to submit a request to the site for review. This is done via the National Centre for Technology in Education's filtering service FortiGuard

6. Blocked Sites:

Although access to social media sites like Facebook, Instagram and Twitter are currently blocked, the school will regularly monitor students' Internet usage.

7. Personal Storage devices:

The use of personal USB memory keys, CD's or DVDs in school requires a teacher's permission and is not advised. The school reserves the right to read all memory devices/disks and to check them for viruses

8. Software Installation:

Uploading and downloading of non-approved software will not be permitted.

9. Downloading:

Downloading by students of materials or images not relevant to their studies is in direct breach of the school's acceptable use policy.

10. Virus protection:

Software will be used and updated on a regular basis.

11. Copyright:

Students must be aware of and comply with copyright issues relating to online learning. E.g., Especially in the areas of music or other media, and will refrain from distributing these in a manner that violates copyright licences.

12. Copyright downloads:

Students cannot upload, download or transmit commercial software or any copyrighted materials belonging to third parties, without necessary licensing permissions.

13. Viruses:

Students must no create or propagate computer viruses or other harmful files.

14. Networks:

Students must not carry out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestions and hinders others in their use of the internet.

15. Plagiarism & Copyright Infringement:

Students will not copy information into assignments and fail to acknowledge the source. Students will not copy work from other students.

16. School Security:

Students are to be aware that usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity for school security and/or for network management purposes.

17. Digital Citizenship:

When using the internet, no one will undertake any actions that may bring the school into disrepute.

Email:

1. Permission:

Students will use approved class email accounts with the permission and the supervision of a teacher. Students will note that sending and receiving email attachments is subject to permission from their teacher.

2. School:

Students should only use school email accounts for all school related communication.

3. Respect:

Students will only use appropriate language, showing respect to teachers and peers at all times.

4. Appropriate Content:

No one will send or receive any material that is illegal, obscene, and defamatory or that is intended cause upset or intimidate another person.

5. Reporting:

Students should report any aggressive or inappropriate behaviour directed at them or others.

6. Account Privacy:

Students must not reveal their own or other people's personal details such as addresses or telephone numbers or pictures when communicating via email.

7. Face-to Face Meeting:

Accessing instant messaging chats is forbidden. Students will never use email or other internet communication methods to arrange a face-to-face meeting with someone outside of school with the exception of Teams or Zoom meetings that are set up by the school authorities.

Social Media & Digital Citizenship:

1. Students will only have access to sites, discussion forums or other electronic communication forums that have been approved by the school.
2. These forums will only be used for educational purposes and will always be supervised. Usernames will be used to avoid disclosure of identity.
3. The school cannot control what Social Media Sites/Social Networking sites students access in their own personal time and for their own personal use, however students should be mindful to behave responsibly at all times as inappropriate online behaviours outside school can often affect the school community. In cases that are deemed necessary, disciplinary measures may be taken against a student in breach of our school policy.

Digital Citizenship & Social Media:

1. Students should only use appropriate language and image on the internet or on any school virtual learning environment.
2. Students should not post inappropriate personal information about her own (or any other persons) life, experiences or relationships.
3. Students should ensure that anything they post online will not put them at risk.
4. Students should never publish full contact details, a schedule their activities or inappropriate personal details in public spaces.
5. Students should report any aggressive or inappropriate behaviour directed at them.
6. Students should not share their passwords or account details with anyone else.
7. Students should show respect to others and not use electronic mediums to upset, intimidate, harass or stalk other people.

School Social Media Accounts:

1. All official school social media accounts are used to promote the school within the wider community and facilitate parents, teachers and students with easy access to the most up to date information about school events and activities.
2. All accounts will be monitored by designated teachers and people wishing to post must liaise with one of these teachers in advance of posting.
3. Photographs, audio and visual clips will focus on group activities and students' activities. The names of students and photographs will only be used for school-related purposes.
4. Any social media accounts, pages, or groups that use the school's name or images without the consent of the principal and/or Board of Management are strictly prohibited.

6. School-Student Social Media Accounts & Acceptable Usage Policy:

Student Leadership & Student Voice:

1. Members of our student council and various student leaders, may operate school twitter accounts.
2. Student must seek permission from the principal before using this account.
3. They must liaise with the Principal to ensure they have a clear understanding of school AUP.
4. All Accounts will be monitored by a named teacher and the author of this account must liaise with this teacher on a regular basis.
5. Photographs, audio and visual clips will focus on group activities and not on individual students. The names of students and photographs will not appear together.
6. Content uploaded is for educational purposes only to promote student achievement.
7. Students will not post material that is illegal, obscene, and defamatory or that is intended to cause upset or intimidate another person.
8. Students will not post content online that may breach copyright regulations or bring the school into disrepute.

Student Personal Devices

The use of mobile/smart phones and all other electronic devices (except when authorised by teachers in a controlled environment such as using laptops or Chromebook, or where a student has reasonable accommodation for use of a digital device) is strictly forbidden.

There are no exceptions to this rule change and there is no discussion to be had. If a parent wants to contact a student for any reason, they must use the correct channels of communication, i.e., through the school office.

Students caught with any device will be **sent home immediately** for the remainder of the day.

1. Tablets/laptops/Phones:

Students using their own technology in school should follow the rules set out in this agreement. Students should only use personal handheld/external devices in school if they have permission. If there is a significant concern about inappropriate usage of their device during this lesson time, a student may be asked to submit their personal device to a teacher, who will in turn hold it and may if necessary, hand to School Management to inspect the search history.

NB Please note students will be responsible for looking after their own devices. In the event of theft, loss or damage the school cannot accept liability

2. Mobile Phones/Smartphones:

- a. As Mobile phones are not allowed to be used within the school generally, they cannot be used within the classroom.
- b. Mobile phones cannot be used at any other time inside the school building.

- c. Students caught with any device will be **sent home immediately** for the remainder of the day.
- d. The unauthorised capture of images, video or audio is in direct breach of the schools AUP.
- e. Connecting or attempting to connect to the school's network system (wired or wireless) without authorisation is in direct breach of the school's AUP.

School Website:

1. The purpose of the school website is to promote the school within the wider community. It will also facilitate ease of access to parents, students, staff and others to the most up to date information on recent events and activities in the school.
2. Material intended for the web site will be gathered, read and approved by the relevant school personnel. An appointed member of staff will gather the materials for use on the school web site, which will then be updated regularly.
3. Photographs, audio and visual clips will focus on group activities and not on individual students.
4. The names and photographs of students will not appear together on the website.
5. Personal student information including, home address and contact details, will be omitted from the school web pages.
6. The permission of parents/guardians of students, staff members and any person whose name or photograph could be published on the website will first be sought before his/her name or photograph is published on the website.
7. Students, staff or others in the school community or associated with it, who publish work on the website will continue to own the copyright on their own work.

Distance learning/Online Learning from home

The same standards of behaviour and appropriate usage will apply to use of the internet or electronic devices to access school materials or classes online from home or other locations outside of the school.

In particular, recording audio or video of classes, taking images during class is strictly forbidden and is a serious breach of the AUP. Students may not disrupt or interfere with online classes in anyway.

For further information on this please consult the Distance Learning Policy.

Further Support Advice & Guidance on Internet Safety:

www.webwise.ie

www.education.ie

www.pdsttechnologyineducation.ie

Support structures :

Where appropriate, the school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the internet.

Reporting on Inappropriate Online Activity:

Students should report all inappropriate activity to the supervising teacher in the room without delay and/or to the respective year head of the student's year group. Under The Harassment, Harmful Communications and Related Offences Act, 2020, it is a criminal offence to distribute, publish or threaten to publish or distribute an intimate image of another person without their consent. If this happens to a student, parents are advised to report immediately to an Garda Síochána. It is also illegal to possess such images of students as this is classed as Child Pornography.

Sanctions for Misuse of Digital Technologies and Internet Usage:

1. Misuse of the Internet may result in disciplinary action, including, in extreme cases suspension or expulsion in accordance with the Code of Behaviour.
2. The school also reserves the right to report any illegal activities to the appropriate authorities.
3. Misconduct will be investigated, and the principal/deputy principal will make recommendations on any report of misconduct with regard to digital technologies and online activity. These recommendations will reflect on whether the incident is considered to be a mild or serious breach and may come with either a mild sanction or heavy penalty respectively in accordance with the relevant policies such as Anti-Bullying and Code of Behaviour.

This Acceptable Usage Policy was adopted by the Board of Management on 3rd October 2023 and will be reviewed on an annual basis.

Signed:



Chairperson of Board of Management

Date: 3rd October 2023

Signed:



Principal/Secretary to the Board of Management

Date: 3rd October 2023

Date of next review: October 2024

