ICT Acceptable Usage Policy (AUP)

St Mary’s Diocesan School is a Catholic Secondary School committed to the development of the whole person, offering equal opportunities to all to achieve their full potential in a familial Christian environment. The school aspires to an education based on high ideals and a broad curriculum which will allow students to confidently play their role in society.

Introduction & Rationale

The Acceptable Use Policy (AUP) is to help to ensure that students become responsible **Digital Citizens** who will benefit from learning opportunities using the school’s ICT resources in a safe and effective manner. These resources support all teaching and learning in the school. The use of IT resources is a privilege and comes with rights and responsibilities. This policy gives guidance and direction for the acceptable use of ICT as appropriate for all members of the school community (i.e., students, staff, and parents/guardians) who have access to, and who are Users, of ICT. It is essential that our school community:

- Takes good care of all school ICT equipment and uses it responsibly.
- Treats other users with respect always.
- Respects the right to privacy of all members of the school community.
- Respects copyright and acknowledge creators when using online content and resources.
- Does not engage in behaviours or misuse ICT resources in a manner that would bring the school into disrepute.

Scope

Students and the wider school community are expected to adhere to all aspects of this policy throughout their time in St Mary’s Diocesan School, Drogheda. This policy covers all types of devices (laptops, one-to-one devices, mobile phones). From September 2024, all incoming 1st year will be using one-to-one devices in classrooms. The school reserves the right to report any illegal or inappropriate activities to the relevant statutory authorities such as An Garda Siochana, TUSLA, and/or the Data Protection Commission. This policy must be read in conjunction with all other school policies, but in particular the following:

- Code of Behaviour
- Anti-Bullying Policy
- Child Safeguarding Statement and Risk Assessment
- Data Protection Policy

Audience & Agreement

All Users of St Mary’s DS, Drogheda IT systems must read, understand, and comply with the contents of this policy.

Guiding Principles & Strategies for ICT Usage

Every time a User enters his/her username & password to use the School’s Network s/he agrees to the following guiding principles:

1. Users will act responsibly.

2. Users will report any damages found prior to use. The school reserves the right to seek compensation for damages to devices.
3. Any violation of these rules will lead to withdrawal of all privileges in relation to ICT.

Our school community adopts several strategies to maximize learning opportunities and reduce risks associated with ICT usage as outlined now:

- Users will be issued with a Schoolwise and Microsoft Office 365 Account which will provide access to Office applications, Outlook Email, OneDrive (cloud storage). Users are strongly encouraged to save everything onto OneDrive as this means files can be accessed from any physical location (i.e., at home, in school etc.). Uses will be given access to accelerated reader app and book publisher apps.
- Users must use their own unique username and password assigned to them.
- St Mary's DS reserves the right to monitor Users' activity to ensure IT resources are being used appropriately and for educational purposes only. Users should also be mindful of copyright infringements and plagiarism when creating & sharing material via OneDrive.
- Users must not create websites, pages, groups, or other social media accounts, which reference the school.
- Users must not create, transmit, display, publish or forward any material that is likely to harass, cause offence to any person or bring the school into disrepute.

Guidelines relating to Specific Aspects of ICT Usage

1. *World Wide Web/Internet Access*

a. Users accessing the internet will be supervised & directed by a teacher in school.
b. Users will not intentionally visit internet sites that contain obscene, illegal, hateful, or otherwise objectionable material.
c. Filtering software and/or equivalent systems will be used to minimize the risk of exposure to inappropriate material.
d. Users will report accidental accessing inappropriate materials to the teacher.
e. Users will use the internet for educational purposes only.
f. Users will not copy information from the internet or AI generators into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
g. Users will never disclose or publicise personal information.
h. Downloading materials or images not relevant to studies is in direct breach of this policy.
i. Users will be aware that any internet usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.
j. Only school Wi-Fi and no other internet can be used on students' one-to-one/ school devices.

2. *Email Communications*

a. Users will only use their approved school email accounts for all school correspondence.
b. Users should not share their usernames and passwords with anyone else and should only use their own.
c. Users should be aware that email is effectively on the school's headed paper and can be traced back to person (sender), place, date, and time of sending.

d. Prior to sending an email the User should ensure that they are satisfied with the content and should doublecheck the address of the intended recipient (to ensure accuracy). Once the ‘send’ key is pressed the email cannot be stopped or retrieved. Deleting mail from your system does not make it untraceable.
e. Users should make sure to ‘address’ the person to whom they are writing the email, write full sentences as part of the communication, and sign-off appropriately. Text-speak is not appropriate within the context of sending an email.
f. Users will not instigate or forward ‘junk’ or ‘spam’ mail to other users either within or outside the school.
g. Users will not send any material that is illegal, obscene, or defamatory or that is intended to annoy or intimidate another person. If users are sent this they should inform the teacher.
h. Users will not reveal their own or other people’s personal details, such as addresses, telephone numbers or pictures.
i. Users will never arrange face-to-face meetings with anyone they only know through emails and/or the internet.
j. Should a User receive material, that is considered offensive or abusive or time wasting than the student should report this immediately to the supervising teacher.

3. *Social Media/Internet Chat*

a. Users must not use social media in any way to harass, insult, abuse or defame any member of the school community, and this applies to both in-school online communication and outside of school online communication.
b. Users will only have access to chat rooms, discussion forums, messaging or other electronic communication if being directed by the Teacher.
c. Face-to-face meetings with someone organized via Internet chat is strictly forbidden.
d. Users must not engage in activities involving social media or any form of communications technology that may bring St Mary’s DS into disrepute.
e. Users must not represent their own personal views as being those of St Mary’s DS on any social medium.

4. *School Website*

a. The school website operates under the authority of the Board of Management and is managed by members of the school staff on behalf of the school.
b. Appropriate permissions are sought on each student in relation to sharing photos/images of students undertaking educational activities to be shared on external platforms. If the school inadvertently displays an image without the appropriate consent it will be removed on the school being made aware of the error.
c. Students may be given the opportunity to publish schoolwork on the school platforms.

5. *Recording of Images/Video*

a. Students must not share images, screenshots, videos, or other content online – of themselves or other students/ staff unless prior permission has been given for educational purposes.

6. *Cyberbullying*

a. St Mary’s DS adheres to the Department of Education & Skills Procedures for Anti-Bullying for Primary and Post-Primary schools and has formally ratified its own policy published on the school website. The accepted definition of bullying is <u>*unwanted negative behaviour, verbal, psychological or physical, conducted by an*</u>

<u>*individual or group against another person (or persons) and which is repeated over time*</u>. This definition includes cyberbullying even when it happens outside the school.

b. Additionally, the posting of an offensive comment online is considered cyberbullying, due to its potential to be circulated to many users. Such incidents of cyberbullying will be dealt with under the school's Antibullying Policy.

c. Students are expected to treat others with respect when using form of communications technology either as part of school-based learning or for personal use outside of school.

d. Engaging in online activities which are harmful or embarrassing towards another student or member of staff is unacceptable behaviour, with serious consequences and sanctions for those involved.

Guidelines relating to Specific Aspects of Digital Devices (iPads, Laptops, Tablets)

1. *One-to-One Devices – General Care & Precautions*
   a. Students are responsible for the general care of whatever device they are using. Devices that are broken or fail to work properly must be taken to a Deputy Principal for evaluation.
   b. Devices should only be used during class time and for homework and not for any other purpose.
   c. Devices must remain in their protective case in the school & at home when not in use.
   d. Students must arrive at school with their device fully charged (>80%). It is the students' responsibility to charge their device and not the schools.
   e. Devices are not to be left unsupervised (for example in an unlocked locker)
   f. Care is to be taken around cables. They should be wound correctly when not in use and removed with care to avoid damaging the charging port.
   g. Devices should not be kept in the same bag compartment as your water bottle. Similarly, water bottles are not permitted on tables during class time.
   h. Use a dry soft cloth when cleaning your screen. No liquid cleanser is necessary.

2. *One-to-One Devices – Screen Care*
   a. Device screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure.
   b. Do not lean on the top of the device when it is closed.
   c. Do not place anything near the device that could put pressure on the device.
   d. Do not 'bump' the device against lockers, walls, car doors, floors etc. as it will eventually break the screen.

3. *Substitution of Equipment*
   If a student's device is not functioning, substitute devices may be issued (depending on availability). If there is no device available, it is expected that students will use hardcopy textbooks in class. If a student receives a substitute device, then they are responsible for the care of this device. If a student damages the substitute device, then the onus to repair will fall on the student/parent/guardian. These repairs must be carried out by a recommended authorised supplier as agreed by the school. If the student forgets to bring in the substitute device or uses the substitute device inappropriately then the student will not receive another device. Students cannot borrow school devices without permission.

4. *Using Your Own Device (Students) (eg mobile phone)*
   a. Students may be granted permission, from time to time, to use a personally owned mobile device within the school for educational purposes only.
   b. Students will always take responsibility for the appropriate use of their personal device. The school is not, in any way, responsible for personal devices.

c. Students, parents/guardians are responsible for their own devices including any breakages, costs of repair or replacement.
d. The school reserves the right to inspect or monitor student mobile devices during school hours.
e. Violations of any school policies or rules involving a student device may result in a student not being allowed continue to use the device during school hours and/or disciplinary action, for a period to be determined by the school.
f. Comply with teachers' requests regarding use of devices during school hours/classes.
g. Mobile devices must be charged prior to bringing them to school as charging mobile devices in school is not permitted.
h. Students may not use their devices to record, transmit or post photos or videos of staff or students. Failure to comply with this will result in serious consequences.
i. The school takes no responsibility for stolen, lost, or damaged devices including lost or corrupted data on those devices.

5. *Shared Equipment*

a. The teacher is in control of and has responsibility for the booking (on vsware), transport to class and safekeeping of devices and students do not have permission to book or take devices without the permission of the teacher.
b. Teachers will make arrangements for the safe transportation of devices to classrooms from the storage point and back to the storage point after (ensuring all devices are plugged in to charge and the box is plugged in at the wall).
c. The teacher will organise for the destitution of devices in class, checking that they are all working on distribution.
d. If there are any devices not working the teacher will report this to the IT coordinator or a deputy principal.
e. The teacher will check that the devices are in the same working order when collecting as when they were given to students.
f. Students should use their own PC login provided and not a generic password unless directed by the teacher. Should another student be logged in when the device is open, the student using the device is responsible for logging that student out.
g. Students should save all work to OneDrive/ the cloud and not to the desktop of the shared device. Students should not delete any saved work on the desktop- but inform a teacher.
h. When finished using, the students should close down all application s and full shut down devices.

Device Responsibilities

1. *Student Responsibilities*
   a. Will arrive to school each day with a fully charged device (>80%)
   b. Will use all devices in a responsible and ethical manner.
   c. Tell teacher if they encounter any problems while using the devices.
   d. Power down the device when finished working on them to protect their work.
   e. Notify your teacher if you receive any inappropriate/ abusive messages.
   f. Will not plagiarize work found on the internet and use for their own purpose. Plagiarism is taking work, that is not your own, and using it as if it was your work.
   g. Will not use any translation tool (such as Google Translate) to produce work in your chosen language that you are studying in class.

h. Will not use any AI tools such as ChatGPT to create work/essays that teachers have assigned for you to complete. Will always protect the rights of copyright owners.
i. Do not allow anyone to use the device other than your parents/guardians.

2. *Parent/Guardian Responsibilities*
   a. Contact Wriggle in a timely fashion to arrange the ordering/payment of your child's device.
   b. Talk to your child(ren) about the values & standards that should be followed when using the internet/devices.
   c. Ensure that you receive all necessary information and sign the relevant forms for Acceptable Usage & Data Protection.
   d. Ensure your child is not engaging in any inappropriate behaviour.
   e. Parents/Guardians should immediately report any damage, interference or issues relating to ownership, possession, or use of the device to a Deputy Principal.
   f. Parents/Guardians should inspect the student's device on a regular basis.
   g. Parents/Guardians should inspect the student's internet history on a regular basis.

3. *School Responsibilities*
   a. Provide internet access at school and provide Users with an academic email account.
   b. Provide internet blocking of inappropriate materials while using devices in school.
   c. Provide staff guidance to aid students in conducting research, academically related activities and how to ensure student compliance of the Acceptable Usage Policy.

Educational Use Only AND Strictly Prohibited Activities

Student use of devices (laptops, iPads, mobile phones, devices) in class is for educational use only. Devices and Laptops are 'managed' devices meaning they are preloaded with educational applications permitted to run on these devices within St Mary's Diocesan School. It will not be possible to download other applications onto these devices.

Parents/Guardians retain ownership and possession of the students' one-to-one device and agree to grant to teachers and school management the right to collect, inspect or confiscate (for a limited period) the device at any time, and the right to alter, add or delete any installed software or hardware. Parents must also agree that the school will manage and monitor the device.

Usage within the school is a privilege and not a right. Students may lose the privilege to use the iPad and to have it in their possession if they abuse their responsibilities and breach this policy. Specifically prohibited activities include:

- Any action that violates existing school policies or public law
- Removal or attempted removal of the Mobile Device Management from the device (this includes attempts to hack or jailbreak a device)
- Taking photos, images, screenshots and/or videos without permission using the device (and / or using the device to circulate same).
- Downloading or attempting to download software/applications that have not been approved.
- Attempting to contact teachers virtually by any other means other than through schoolwise, Microsoft teams and/or Microsoft outlook.
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, sexually explicit or criminal materials.
- Playing internet/computer games in class without permission.
- Spamming – the act of sending mass emails to other students/staff.
- Gaining access to other members' school accounts, files/personal data.
- Use of communications to mislead, harm, bully or harass another person is strictly prohibited.

- Any use of a proxy server or Virtual Private Network (VPN) i.e. as a tunnel bridge to access sites.
- Bullying of any kind as defined by the St Mary's Diocesan School Anti-Bullying Policy will not be tolerated.

Inspections
Students may be selected, at random, to provide their devicef or inspection. If a student's device is requested for an inspection, students must unlock the device. St Mary's Diocesan School reserves the right to confiscate any device. The device will be inspected, and it may be kept until such time as school management arranges a meeting with a parent/guardian to come in and collect it.

Remote Learning Student Conduct & Protocols

Protocols are in place to ensure the staff and students at St Mary's Diocesan School, Drogheda can continue to learn in a remote environment, when circumstances dictate that this must take place. This policy is designed to provide continuity for staff and student engagement in a remote learning environment that utilises existing systems and processes. Note that the recommended platform for all Users is Schoolwise, Microsoft 365 (this includes Outlook Email, OneDrive, OneNote, and Microsoft Teams). In addition to this publishing apps/ sites may be used.

Remote Learning Student Conduct & Protocols

1. *Student Expectations & Conduct*

   a. Students are expected to continue and participate in learning activities and to complete work within designated timeframes as guided by their teachers.
   b. Students are expected to commit – as closely as possible - to a learning duration that reflects what would normally happen within the context of being physically in school.
   c. Students are expected to be respectful, thoughtful, and kind in all online communications with peers and teachers.
   d. When participating in 'online classes' or 'live sessions' with teachers and classmates it is expected that students will:
      i. Be dressed appropriately and sitting in an appropriate location in front of their device
      ii. Be on time for the session and courteously quiet while waiting for other class members to join the session
      iii. Follow instructions from the teacher to minimise any unnecessary noise during the session
      iv. No eating or drinking during online live classes.
      v. When you have a question wait for your teacher to call on you.
      vi. Stay attentive and follow what your teacher and other students are saying.
   e. Students are expected to behave 'online' in the same manner as would be expected in the classroom. Any recording video or taking pictures of either the teacher or students while participating in online/live sessions is strictly prohibited.

2. *Teacher Commitment*

   a. Teachers are expected to provide work and guidance to classes as well as to support all of their students recognizing that not all students will have the same access to devices and/or will have the same available time due to other commitments in the home

b. Teachers are expected to communicate with students using school email communications and/or Microsoft Teams/ Schoolwise. Work should be provided in manageable chunks with reasonable deadlines along with what the sanctions are if work is not completed or submitted on time.
c. Teachers are expected to be available for students during school hours. Teachers will maintain their own records in relation to online engagement/non-engagement. Patterns of non-engagement will be escalated to the Year Head for action and will be processed/managed through the Care Team structure.
d. Teachers will follow the same protocols in dealing with bad behaviour in an online setting as happens in the context of the classroom.

Sanctions for the misuse of ICT and Internet

The misuse or unlawful use of the Internet or ICT equipment/resources by Students will result in disciplinary action as outlined in the school's Code of Behaviour and Anti-Bullying Policy. Sanctions will include withdrawal of access and privileges to ICT and other school-related privileges and, in extremely serious cases, sanctions up to and including expulsion. The school also reserves the right to report any illegal or inappropriate activities to the relevant statutory authorities such as An Garda Siochana, TUSLA and the Data Protection Commission.

Legislation

The following legislation is relevant to Internet Safety but is not exhaustive:

Data Protection Act 2018 – this act gives effect to the General Data Protection Regulation (GDPR) in the Irish context.

Data Protection Act 1998 – this act was passed to deal with privacy issues arising from the increasing amount of information being kept electronically on individuals.

Data Protection (Amendment) Act 2003 – this amendment extends the data protection rules to manually held records and makes improvements to the public's right to access data.

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.

Interception Act 1993 – this act stipulates that telecommunications messages can be intercepted for the purpose of an investigation of a serious offence. Authorizations are subject to certain conditions.

Video Recordings Act 1989 – this act prohibits the distribution of videos which contain obscene or indecent materials which may lead to the depravation or corruption of the viewer.

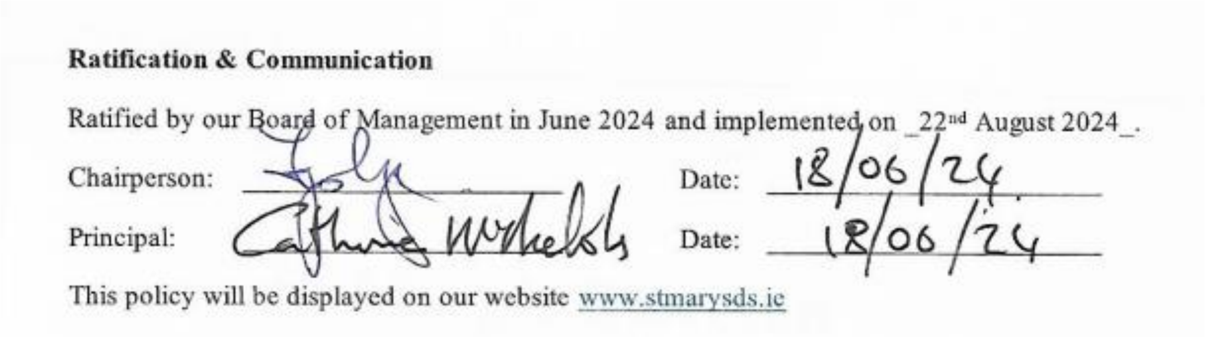
Copyright and Related Rights Act 2000 – this act governs copyright in Ireland.

Internet Safety Advice – additional resources

Useful websites for further information on online and communications technology:

www.webwise.ie (information on various forms of internet usage)
https://cybersafeireland.org/ (promotes and provides education to ensure safe and responsible navigation of the online world)

https://spunout.ie/ (how to protect your privacy and security online)
https://savvycyberkids.org/ (educating and empowering Digital Citizens)
www.connectsafely.org/cyberbullying
www.esafety.ie (Internet Safety Seminars for Schools/Parents)



Ratification & Communication

Ratified by our Board of Management in June 2024 and implemented on _22nd August 2024_.

Chairperson: ____________ Date: 18/06/24

Principal: ____________ Date: 18/06/24

This policy will be displayed on our website www.stmarysds.ie

Monitoring and Review

This policy will be monitored on an on-going basis and will be reviewed and amended as the need arises.

Student & Parent/Guardian Acceptance of the ICT Acceptable Usage Policy

STUDENT ACCEPTANCE

Please review the School's ICT Acceptable Usage Policy. Having done so, please sign this form to provide a written record that you have read, understood, and agreed to the terms of this policy. If you do not understand or are unhappy with any part of this policy, please contact the school.

Student's Name: ____________________________

Student's Signature: ____________________________

Date: ____________________________

PARENT/GUARDIAN ACCEPTANCE

As the parent or legal guardian of the above student:

- I confirm that I have read the ICT Acceptable Usage Policy and accept the terms.

Parent/Guardian Name: ____________________________

Parent/Guardian Signature: ____________________________

Date: ___________________________