St. Mary's Secondary School,
Holy Faith, Glasnevin, Dublin 11.
60770P

Acceptable Use Policy

Dates for Review

Staff	**?**	**Reviewed**
Parents	**?**	**Reviewed**
Student Council	**?**	**Reviewed**
Board of Management	**?**	**Ratified**

Table of Contents

Introduction

Access to Information and Communications Technology (ICT) in a school setting provides the staff and students of St. Mary's with the benefits of enhanced teaching and learning opportunities. It is through this lens that St. Mary's Acceptable Use Policy (AUP) has been drawn up. The sole aim of this policy is to ensure that the digital resources that are provided by the school can be used in a safe and supported manner. The use of ICT in St. Mary's is a fundamental part of the school's digital strategy, whereby students and staff should be able to access appropriate hardware, software and internet resources to help them teach, learn, create and communicate during their time in school. This approach is encouraged and supported by the government's Digital Learning Framework.

The AUP applies to students who have access to and use the ICT resources provided by the school. It also applies to members of staff, volunteers, parents, and others who access the school's digital resources.

Access to ICT resources is considered a school privilege. Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions will be imposed.

It is envisaged that school and parent representatives will revise the AUP annually. Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

Access to ICT in St. Mary's

In St. Mary's, all staff and students are given a school username and password for accessing the MS Office 365 platform. They will use this account for communication, collaboration and storage during their time in the school, using software such as Outlook, SharePoint, OneNote and Teams. These accounts are controlled and restricted by the school.

Staff and students will also have access to school-owned devices. School usernames and passwords must be used, in order to log on to this school device. Restrictions apply to their use, which prevent the downloading of software and access to specific websites. Upon leaving St Mary's, staff will be asked to return their school device on the date that they officially leave the school.

Staff and students must use their MS Office 365 account to store their school-based files. Such files should not be stored on any school-owned device, as any electronic material stored on school-owned devices may be deleted without notice at any time. The use of USB keys on school-owned devices is strictly prohibited.

All student mobile phones must be switched off on entry to the school grounds and kept on the student's person, preferably in their zipped pocket. Students are not permitted to use their mobile phones during the school day, unless required to do so for teaching and learning purposes and only when teacher permission has been given (See our Mobile Phone Policy

2020). Students may also be permitted to turn on their phones when signing in late or leaving early using the Digital Sign In/Sign Out System at reception.

Promoting Acceptable Use in St. Mary's

The following strategies have been implemented in St. Mary's to maximise teaching and learning opportunities and reduce risks associated with ICT resources:

- Provision of internet safety advice and support opportunities to students in St. Mary's through our annual Cyber-Safety Week for all students, our Induction programme for all incoming students and our SPHE and Wellbeing classes provided at Junior Cycle
- Provision of Continuous Professional Development (CPD) to teachers as the need arises
- Promoting an ethos of respect at all times among staff and students and a commitment not to undertake any actions that will bring the school into disrepute
- Supervision of students when using ICT resources during class time and when in the Computer room
- Monitoring students' internet usage if necessary
- Prohibiting the uploading and downloading of non-approved software
- Use of a government approved web filter to minimise the risk of exposure to inappropriate material
- Use and regular update of virus protection software on all school computers
- Seeking parental permission if publishing content on the school website and/or school social network that focuses on individual students
- Use of MS Office 365, as well as other school approved communication platforms such as the School App, Twitter, Edmodo and Kahoot, when communicating with students, parents and other stakeholders.

Responsibilities and Expectations

In using digital technologies and internet resources in our school, we are expecting that all users will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute. Neither social media nor the internet may be used in any way to harass, insult, abuse or defame students, their family members, staff or other members of the school community. Specific expectations have been outlined below:

1. **Staff and Student Digital Accounts**

Staff and students of St. Mary's have been issued with ICT accounts. The school retains ownership of all data and services arising from these accounts. However, all staff and students are responsible for all activities and information accessible through their school account. In order to ensure the correct use of school-owned digital accounts, it is expected that:

- School accounts will be used for approved school-related communication. School e-mail addresses will be used for communication among staff members and between students and teachers

- Students only have permission to use their school accounts for websites and for communication approved by the school, for educational purposes
- To prevent computer viruses being transmitted through the system, there should be no unauthorised downloading/installing of any software
- In exceptional circumstances, permission may be given by teachers to students to access personal email accounts or messaging services for a fixed purpose e.g. accessing a particular file
- Personal details including passwords, mobile numbers or home addresses should not be revealed to others
- School email accounts should not be used to register for online services such as social networking services, apps, and games
- It is the user's responsibility to make sure that they sign out of their MS Office 365 account after use and to never leave it unattended when signed in
- Accounts will not be used to engage in online activities such as uploading or downloading large files that result in heavy network traffic, which impairs the service for other internet users
- Staff and students must use their MS Office 365 account to save their files. Such files should not be stored on any school-owned device, as any electronic material stored on school-owned devices may be deleted without notice at any time
- Any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person will not be sent or received
- Students should immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Students should avoid opening emails that appear suspicious. If in doubt, students should ask their teacher before opening emails from unknown senders
- Information stored on the MS Office 365 platform may be accessed by the school in matters relating to serious misconduct. Any breach of the AUP will be dealt with according to the Ladder of Referral as outlined in the school's Code of Behaviour.

2. Internet Use

In order to ensure safe access to the school's Wi-Fi network, it is expected that all staff and students adhere to the following guidelines:

- The Internet will be used for educational purposes only
- Websites that contain obscene, illegal, hateful or otherwise objectionable material will not intentionally be visited
- Accidental accessing of inappropriate materials will be reported in accordance with school procedures
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement)
- Personal information will never be disclosed or publicised online
- Students will not download materials or images that are not relevant to their studies

- Students will be aware that any usage, including distributing or receiving of information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons
- Appropriate social behaviour in the online environment, which is courteous and respectful is expected at all times
- It must be recognised that among the valuable content online, is also unverified, incorrect, or inappropriate content. Trusted sources should be used when conducting research via the Internet
- Students should not post anything online that they would not want parents, teachers, or future colleges or employers to see.

3. Publication of Student's Work and Images

Student's work and images may be published on school-based platforms throughout the school year. In doing so, it is expected that:

- Parent/guardian permission is sought to publish photographic and video images of students on a variety of school-based forums, including the school website, our social media accounts, the school newsletter and the yearbook
- Students have sought their teachers' approval when publishing projects, artwork and other schoolwork through school-based platforms
- Any student work which is published online will appear in an educational context with a copyright notice prohibiting the copying of such work without express written permission
- Students will continue to own the copyright on any work created under their school account and/or published on the school's communication channels
- Content focusing on individual students will at times be used for the purpose of SLAR (Subject Learning Assessment Review) meetings.

4. Remote Teaching and Learning

ICT provides staff and students with many teaching and learning opportunities. In the case of remote teaching and learning, it is expected that the following guidelines will be adhered to:

- Staff and students use our nominated platform MS Office 365 Teams, as well as other school approved communication platforms such as Edmodo and Kahoot for remote teaching and learning. The online collaboration system MS Office 365 provides our students and staff with access to a secure online web-based storage space (One Drive), a St. Mary's e-mail account, and access to MS web-versions of Word, Excel, PowerPoint and OneNote
- MS Office software may also be downloaded and used on home or personal Mac or Windows PC, as well as iPad/iPod/iPhone or Android mobile devices, using a St. Mary's email address
- MS Office 365 is not for student personal records. No student home address information, health, medical, behavioural or welfare information will be stored in MS Office 365

- The access rights associated with your MS Office 365 account may be changed or revoked should your status as an employee or student change/terminate
- Upon leaving St. Mary's, staff and students' MS Office 365 accounts will be retained for one month after the start of the next school year or for one calendar month if leaving in the middle of a school year. After this date, all associated accounts will be inaccessible and related data will be deleted
- Only students are permitted to join MS Teams classes. Below is a list of the school rules pertaining to MS Teams classes:
  - ✓ Student cameras and microphones should be turned off for the class duration unless requested otherwise by a teacher
  - ✓ Students are not permitted to record MS Teams lessons on any device
  - ✓ The 'chat' function in MS Teams is limited to content on teaching and learning only
  - ✓ Communication on the Teams Class Platform is restricted to the student and the teacher.

5. Cyberbullying

The cyber safety of all our students is of paramount importance and any incidences of cyberbullying will be strictly dealt with in line with our Code of Behaviour and our Anti-Bullying Policy. Cyberbullying involves unwanted messages, images, audio or video sent by electronic means to threaten abuse or harm someone. This definition of cyberbullying is also considered to be bullying, even when it happens outside the school or at night. When using the school's digital resources, the following points apply:

- Students, parents and staff are expected to treat others with respect at all times
- Engaging in online activities with the intention to harm, harass, or embarrass another student or member of staff is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved
- Placing a once-off offensive or hurtful public message, image or statement on a social network site or other public forum where that message, image or statement can be viewed and/or repeated by other people is also regarded as bullying behaviour
- The prevention of cyberbullying is an integral part of the Anti-Bullying Policy of our school.

6. Parental Responsibilities

We would encourage parents:

- To research the minimum age requirements for different social media sites and not allow their child to have an account until they are the appropriate age
- Not to 'tag' photographs or any other content which would identify any students or staff in the school on their social media sites
- To ensure that online messages and comments to the school are respectful. Any messages written on social media are treated in the same way as written messages to the school

- Avoid any negative conversations about students, staff or parents on social media accounts. Comments of this nature will be deleted
- Not to request to ‘friend’ a member of staff in the school.

7. Legislation

Upon request, the school will provide information on the following legislation relating to the acceptable use of the internet. We would advise all teachers, students and parents to familiarise themselves with:

- Data Protection Act 2018
- Child First Act 2015
- Child Trafficking and Pornography Act 1998
- Interception Act 1993.

8. Sanctions

The school’s Code of Behaviour underpins and supports this Acceptable Use Policy. To this end:

- Misuse of the school’s hardware, software or internet access may result in disciplinary action, in line with the Code of Behaviour. The school also reserves the right to report any illegal activities to the appropriate authorities.
- If a student is found in violation of the school’s AUP, their school accounts may be suspended or restricted to prevent specific actions. The school has full control over what applications each account holder may use

9. Access to Individual Accounts by the School

Information stored on a school-based account may be accessed by the school or by a parent/guardian, if the user has, or is suspected to have violated the school’s AUP. The access to this information is treated seriously by the school. The Principal and Deputy Principals are the only members of staff with the authority or administrative rights to access this information created through their MS Office 365 account. A formal procedure will be strictly followed on any occasion where student information needs to be accessed by the school. This procedure is laid out below:

- A parent/guardian or teacher will need to write a letter explaining the reason a student’s information needs to be accessed
- The parent of the student whose account is to be accessed, will be notified and given the opportunity to be present when the information is being accessed
- The student’s account information will be accessed through the digital archive and exported while at least two school administrators are present
- Any information, which is relevant to the initial complaint, may be used by Senior Management to determine if the Code of Behaviour was breached.

This AUP and its implementation will be reviewed regularly by the following stakeholders:

- Board of Management
- Staff
- Students
- Parents/guardian

Ratified by the Board of Management on: 11th June 2020

Signature: Audrey Doyle

Audrey Doyle
Chairperson
Board of Management

APPENDIX A

St. Mary’s Secondary School

Student Acceptable Use Policy Agreement

I ____ (name and class) agree to follow the school’s Acceptable Use Policy on the use of Digital Technologies and Internet Access. I will use all Information and Communication Technology in a responsible way and adhere to all the rules in the policy, explained to me by the school.

Student’s Signature: ____________________ **Date: ____________**

Parent(s)/Guardian(s) Acceptable Use Policy Agreement

I/We ____ the parent(s) or guardian(s) of the above student, have read the Acceptable Use Policy and grant permission for my child to use Information and Communication Technology and access the Internet. I understand that Digital Technology use and Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if students access unsuitable websites.

I accept the above paragraph ___ / I do not accept the above paragraph ___

(Please tick as appropriate)

Signature(s): ______________________________ Date: __________________