

# ICT Acceptable Use Of Information and Communications Technologies (ICTs) Policy



Scoil Bhríde Mercy Secondary School

Review of AUP completed: June 2021

## Introduction

The school provides access to various computer resources, including the school network and the internet. These resources are available to facilitate the learning process in a supportive school environment and to provide quality learning outcomes for our students. The school encourages students to become familiar with the use of information technology in the achievement of learning outcomes and personal learning goals.

The aim of this policy is to ensure that pupils will benefit from learning opportunities by the school's internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school policy is not adhered to this privilege may be withdrawn and the appropriate sanctions will be imposed. This policy updates all previous school AUP policies

## Definitions

- AUP: Acceptable Use Policy
- ICT: Information Communication Technologies (devices)
- GSuite (is the suite of resources made available by Google: Gmail, Chrome, Google Classroom etc.)
- Hardware: Physical parts of a computer e.g. monitor, mouse and keyboard
- Operating System: Software that manages the resources of a computer and allows the application software to run.
- Applications Software: Programmes that run on a computer, e.g. word, spreadsheets.
- Server: A powerful computer that controls access to all other computers.
- Internet: Worldwide connected network of computers used to share information.
- WWW: World Wide Web can be considered a virtual library of information.
- Email: Electronic Mail.
- Wi-Fi: Wireless fidelity. Data is exchanged between devices wirelessly.

## Rationale for this policy

This policy is intended to give guidance and direction for the acceptable use of ICT as appropriate for all members of the school community (i.e. students, staff, parents and approved visitors/speakers etc.) who have access to, and who are users, of the School's ICT including but not limited to: GSuite network and the school's Local Area Network (LAN).

When using GSuite, Zoom any ICT, and Compass in Scoil Bhríde, all members of the school community are expected:

- To take good care of all school ICT equipment and use it responsibly in accordance with school policy.
- To treat other users with respect at all times.
- To respect the right to privacy of all members of the school community.
- To respect copyright and acknowledge creators when using online content and resources.
- Not to engage in behaviours or misuse ICT resources in a manner that would bring the school into disrepute.

## **Scope of Policy**

Students are expected to adhere to this policy throughout their time with us as students of Scoil Bhríde.

The school also reserves the right to report any illegal or inappropriate activities to the relevant statutory authorities i.e. Gardaí, TUSLA. Office of the Data Protection Commission etc.

This policy must be read in conjunction with all other school policies including;

- GDPR Policy
- Child Protection Policy
- Code of Positive Behaviour
- Anti-Bullying Policy
- Mobile Phone Policy

## **Acceptable Use Policy for Students**

Every time a student enters a username and password in order to use the School's Computers, GSuite Network, email, Google Classroom, Google Meets, Zoom and Compass she agrees to the following rules:

- Students will report any damages found prior to use. The school reserves the right to seek compensation for damages to computers.
- Students will act responsibly when using computers. All gaming and social networking sites are NOT permitted unless instructed to use by a teacher.
- The student understands that computer sessions will be monitored via classroom control software.
- Any violation of the above in the computer room will lead to restorative action by the school Management with potential for sanctions in line with our code of behaviour

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with ICT. These strategies are as follows:

### **General**

- Students must use their own username and password assigned to them by the school when using GSuite and our ICT equipment.
- All students will be issued with a GSuite package. This will provide access to Google (GSuite) applications such as email (mercytuam.com), cloud storage, communication and collaboration platform (Googlemeets, Google Classroom and Zoom) and video streaming service. Students are encouraged to save their work to their GSuite or google classroom account rather than on the school network or on personal devices.
- Access to the GSuite package will be withdrawn when a student leaves the school.
- The school reserves the right to monitor students' activity on GSuite to ensure that it is being used appropriately and for educational purposes only. Students should seek permission from their teacher before sharing any content using their GSuite account with another member of the school

community. Students should also be mindful of copyright infringements and plagiarism when sharing material via GSuite. Please note activity of users on GSuite is automatically recorded by the system. Reports of user activity are available to school management.

- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
- Students must not create websites, pages, groups or other social media accounts, which reference the school, to express personal opinions without the prior approval of school management. Students 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. Scoil Bhríde reserves the right to protect the reputation of the school.

### **World Wide Web**

- Internet sessions in the school will be monitored using internal software
- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful, or otherwise objectionable materials.
- Filtering software and/or equivalent systems will be used in the school in order to minimise the risk of exposure to inappropriate material.
- Students will report accidental accessing of inappropriate materials in accordance with school procedures via your teacher or Year Head.
- Students will use the Internet in the school for educational purposes only.
- 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.
- Downloading materials or images not relevant to their studies, is in direct breach of the school's Acceptable Use Policy.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

### **Email**

- Students will only use their approved school Gmail (mercytuam.com) accounts for school correspondence.
- Students should be cognisant that Gmail can be traced back to place, date, and time of sending.
- Prior to sending an email, students must ensure that they are satisfied with the content and should double check the address of the intended recipient. Once the "send" key is pressed, the e-mail cannot be stopped or retrieved. Deleting mail from your system does not make it untraceable.
- Students will not instigate or forward "junk mail" to users either within or outside the school
- Students will not send or receive any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

- Students will not reveal their own or other people's personal details, such as addresses, telephone number or pictures.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.
- Should a student receive material, which she finds offensive or abusive or time wasting she should immediately report it to the supervising teacher.
- Students should be mindful of the security of their accounts. Should a suspicious email be received, the incident should be reported to their teacher or Year Head.

### **Internet Chat**

- In the school, students should access to discussion forums, messaging or other electronic communication that have been approved by their teacher.
- Discussion forums and other electronic communication forums will only be used for educational purposes and will be monitored.
- Face-to-face meetings with someone organised via Internet chat is forbidden.

### **School Social Media/Website**

- The school website and social media accounts operate under the authority of the BOM and is managed by members of the school staff on behalf of the school.
- The school Twitter, Instagram and Facebook accounts post regular updates of school news, notices, and activities. Scoil Bhríde also retweets relevant information to other twitter users as appropriate. Permission is obtained from parents/ guardians at enrolment to allow photographs of their daughter to be published on the school website.
- The school YouTube and Zoom channel hosts videos of school activities and performances.
- Students should alert their teacher if they/or their parents do not wish for them to be part of a video or photograph which may may be used on the school website or social media.
- If the school inadvertently displays an image without the appropriate consent it will be removed immediately on the school being made aware of the error.
- Students may on occasion be given the opportunity to publish schoolwork on the school website.
- Personal student information including home address and contact details will be omitted from school web pages.
- The school will ensure that image files are appropriately named.

### **Recording of Images & Video**

- Students must not share images, videos, or other content online which could be deemed harmful to another member of the school community either in school or out of school. Recording of online classes is strictly prohibited.
- Classes recorded by teachers and made available to students are to remain the property of the teacher and Scoil Bhríde. They must not be viewed, downloaded, shared, published, or distributed without the permission of the teacher and school management.
- The school permits the recording of images and videos of students at some school activities once permission has been sought and granted. Students may only take photos or videos on school grounds or when participating in school activities using the school digital cameras as directed by a teacher.
- Students must not take, use, share, publish or distribute images of any member of the school community except with the permission of the teacher and member of the school community.

### **Use of teleconferencing**

- Our school utilises teleconferencing during periods of school closure. Distance learning is a way of learning remotely without being in regular face-to-face contact with a teacher in the classroom. There are many benefits to teaching and learning in this way, and students and teachers have the tools and expertise to use teleconferencing to sustain learning.

- Our school provides a video conferencing option within Google Classroom for our students and staff. It is expected that students and staff will use the platform in a professional and ethical manner for the purpose of teaching, learning and assessment.
- The use of teleconferencing requires students observe the following rules in order to ensure that both staff and students benefit from this way of teaching and learning. Students must not:
  - Post, stream or transmit any content, including live video, that violates this Policy in such a way that is offensive to students / staff.
  - Do anything illegal, facilitate any illegal activity, or promote violence.
  - Do anything that threatens, exploits, or otherwise harms others.
  - Engage in any activity that is harmful, obscene, or indecent. This includes offensive gestures, displays of nudity, violence, pornography, sexually explicit material, or criminal activity.
  - Engage in any activity that is fraudulent, false, or misleading.
  - Engage in any activity that is defamatory, harassing, threatening or abusive.
  - Store or transmit any data or material that is fraudulent, unlawful, harassing, libellous, threatening, obscene, indecent, or otherwise inappropriate.
  - Send unauthorized messages or irrelevant material.
  - Misrepresent a user's identity or affiliation with any entity or organisation or impersonate any other person.
  - Harvest, collect, or gather user data without consent. This includes screen recording or taking screenshots during online classes.
  - Violate or infringe any intellectual property or proprietary rights of others, including copyrights.
  - Violate the privacy of others or distribute confidential or personal information of others.
  - Facilitate access of third parties to school teleconferencing

## **Cyberbullying**

Cyberbullying is a form of bullying which is carried out through an internet service such as e-mail, chat room, online social networking or instant messaging. It can also include bullying through mobile phone or any apps that can be used on their phone, i.e. texting, instant messaging, sending of images etc. (Please note bullying is repeated aggression over time).

Examples of cyberbullying behaviour are:

- Teasing and being made fun of
- Spreading of rumours online
- Sending unwanted messages
- Defamation

## Impact of Cyberbullying and Advice to Students:

Cyberbullying, like all bullying can have terrible effects on those experiencing it. It can lower your self-esteem and you may feel alone, sad, angry and scared. If you are being bullied it is not your fault and there is nothing wrong with you. Don't be afraid to tell someone you are being bullied.

### What to do:

- If you are being cyberbullied keep a record (including time and date) this may help you (or the school) to find out who is sending the messages.
- Tell some – talk to someone you trust, a parent, a friend, school counsellor, chaplain or teacher.
- Contact your mobile phone or internet service provider and report what is happening – they can help you block messages or calls from certain senders.
- Don't reply to bullying messages – it may get worse if you do.

## Responsible Internet Use

These rules will help us to be fair to others and keep everyone safe.

1. I will ask permission before using the Internet.
2. I will not look at or delete other people's files.
3. I will not bring software or external hard drives such as USB sticks into school without permission.
4. I will only e mail people I know, or my teacher has approved.
5. The messages I send will be polite and sensible.
6. I will not give my home address or phone number, or arrange to meet someone.
7. I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
8. I will not use Internet chat.
9. If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
10. I understand that the school may check my computer files and the Internet sites I visit.
11. I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

## Bring Your Own Device

- Some students may be granted permission to use a personally owned mobile device within the school for educational purposes only. Use of a personally owned mobile device will be supervised and will only be permitted during class time. The school will decide on the type of allowed device allowed.
- Students must take responsibility for appropriate use of their personal device at all times. The school is not responsible in any way for personal the devices or for its use.
- Students/parents/guardians are responsible for their devices, including any breakages, costs of repair, or replacement.
- The school reserves the right to inspect or monitor student mobile devices during school hours.
- Violations of any school policies or rules involving a student device may result in a student not being allowed continue using the device during school hours and/or disciplinary action, for a period to be determined by the school.
- During school hours students are allowed use their device for learning related activities only.



- Students must comply with teachers' requests regarding use of devices during school hours.
- Mobile devices must be charged prior to bringing them to school in order so as to be usable during school hours. Student use of charging devices in the school is not permitted.
- Students may not use the devices to record, transmit or post photos or video of other teachers or students. No images or video recorded at school can be transmitted or posted at any time without the supervising teacher's permission.
- Each user is responsible for her/his own device and should use it responsibly and appropriately. The school takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices.
- Scoil Bhríde is not responsible for any possible device charges to your account that might be incurred during approved school-related use

### **Sanctions for the misuse of ICT and Internet by students**

The misuse or unlawful use of the Internet or ICT equipment during school /class time by students will result in disciplinary action as outlined in the school's Code of Behaviour, Anti Bullying Policy, and Mobile Phone Policy. Sanctions may include withdrawal of access and privileges to ICT and other school related privileges and, in extremely serious cases, suspension or expulsion.

GSuite access may be withdrawn for a specified time.

The school also reserves the right to report any illegal or inappropriate activities to the relevant statutory authorities i.e. Gardaí, TUSLA. Office of the Data Protection Commission etc.

### **ICT and Legislation - the following legislation is relevant to Internet Safety.**

Data Protection Act 2018- this act augments the General Data Protection Regulation (GDPR) May 2018 in the Irish context.

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 telecommunication messages can be intercepted for the purpose of an investigation of a serious offence. Authorisations are subject to certain conditions.

Video Recordings Act 1989 - this act prohibits the distribution of videos which contain obscene or indecent material which may lead to the devaluation or corruption of the viewer.

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

## **Student and Parent/Guardian Acceptance of Acceptable Use ICT Policy**

Please review the School's ACCEPTABLE USE OF ICT POLICY. Having done so, please sign this form to provide a 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. Otherwise, tick the boxes next to each statement and sign below.

- I confirm that I have read and understand this IT Acceptable Use Policy
- I agree to abide by the conditions set out in this policy.
- I understand that when I have given consent, my schoolwork, photo or video may be chosen for inclusion on the website, school twitter account or school YouTube or Zoom channel.

Student's Signature: \_\_\_\_\_

Print Name: \_\_\_\_\_

Date: \_\_\_\_\_

## **Support Structures**

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

## **School Strategy**

The school will employ a number of strategies to maximise learning opportunities and reduce risks associated with the internet. These strategies are as follows:

- Internet sessions will always be supervised by a teacher.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor students' internet usage.
- Students and teachers will be provided with training in the area of internet safety.
- Uploading and downloading of inappropriate software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of portable memory devices such as USB memory sticks, SD cards or external hard drives in school requires a teacher's permission.
- Students will observe good etiquette on the internet at all times and will not undertake any actions that may bring the school into disrepute.
- Students are prohibited from using the I.T. resources to engage in bullying tactics.
- Students may not load or play computer games on school computers unless directed by a teacher.
- Whilst limited access social networks is available in Scoil Bhríde, students are not permitted to access them unless under the supervision of a teacher who has given permission to use social networks.

## **School Website**

- Pupils will be given the opportunity to publish projects, artwork or school work on the World Wide Web.
- The publication of school work will be co-ordinated by a teacher.
- Pupils' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
- Personal pupil information including home address and contact details will be omitted from school web pages.
- Pupils will continue to own the copyright on any work published.
- The website will be regularly checked to ensure that there is no content that compromises the safety or pupils or staff.

## **World Wide Web**

- Students will not intentionally visit internet websites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will report accidental accessing of inappropriate materials. If a student accesses inappropriate information they should immediately tell the teacher, the ICT-coordinator, the Principal or the Deputy Principal. This will protect against a claim that this policy has intentionally violated.

- Students will use the internet for educational purposes only.
- Students will be familiar with copyright issues relating to online learning.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement). Students will not plagiarise works they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting it as your own.
- Students will never disclose or publicise personal information.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security, and/or network management reasons.

### **Email**

- Students will use approved class e mail accounts only and under supervision by or permission from a teacher.
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses, personal telephone numbers or pictures.
- Students will never arrange a face-to-face meeting with someone they only know through e mails or the internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.
- Newsgroups will not be made available to students unless an educational requirement for their use has been demonstrated.

### **Netiquette**

- Students will not engage in abusive language while communicating online nor participate in "spamming" i.e. maliciously forwarding inappropriate mails to other I.T. users.
- Students will observe good "netiquette" at all times and will not undertake any actions that may bring the school into disrepute.

Ratified by BOM June 2021