**Acceptable Use Policy**

The Acceptable Use Policy ("AUP") was reviewed in 2012 and subsequently reviewed again in September 2020.

This review was led by the Post Holder with responsibility for IT in conjunction with Staff and representatives of the Parent-body.

This policy is to be read in conjunction with our Anti-bullying policy which also deals with the issue of cyber-bullying.

**Policy Aim**

The aim of this Acceptable Use Policy is to ensure that pupils will benefit from learning opportunities offered 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 Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions, as outlined in the AUP, will be imposed.

It is envisaged that the school and representatives of the parent body will revise the AUP regularly in line with developing technological issues. The AUP should be read carefully to ensure that the conditions of use are accepted and understood.

**Rationale**

The Internet is a valuable teaching and learning tool. The Internet and digital media can help our pupils learn, create and communicate. The online world is very much part of their lives, they are “growing up digitally” with technology embedded in every aspect of their lives. Digital literacy skills are key life skills for children and young people today. They need to be media savvy and know how to effectively search for and evaluate online content; know how to protect personal information and reputation; know to respect copyright and intellectual property and know where to get help if problems arise. It can develop children’s independent research skills and promote lifelong learning. The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. The absolute need for online safety is reinforced at every given opportunity across the curriculum

Information is available on the Internet on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

* Data Protection (Amendment) Act 2003
* Child Trafficking and Pornography Act 1998
* Interception Act 1993
* Video Recordings Act 1989
* The Data Protection Act 1988
* GDPR (EU) (2016)

**Security**

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

 Access to Computers is strictly confined to the Principal, Teaching Staff, S.N.A.s, Childcare Workers, Secretary and children who are under teacher supervision. Any person other than the above named people requires the permission of the Principal/ B.O.M. before using the computers.

* Computer/Internet access by children in school will always be supervised by a teacher or SNA
* The Broadband connection in the school is provided by the Department of Education and Skills (DES) and uses high quality Content Filtering to minimise the risk of exposure to inappropriate websites or material. For more information go to [www.pdsttechnologyineducation.ie/en/Technology/Schools-Broadband/Content-Filtering/](http://www.pdsttechnologyineducation.ie/en/Technology/Schools-Broadband/Content-Filtering/)
* The school will regularly monitor pupils’ Internet usage.
* Students and teachers will be provided with training and information in the area of Internet safety.
* Uploading and downloading of non-approved software will not be permitted.
* Virus protection software will be used and updated on a regular basis.
* The use of memory sticks or other digital storage media in school requires a teacher’s permission.
* Students will observe good “netiquette” (etiquette in the internet) at all times and will not undertake any actions that may bring the school into disrepute.

**Use of the Internet**

* Students will use the Internet in school for educational purposes only.
* Webwise Internet Safety [www.webwise.ie](http://www.webwise.ie) guidelines are used as a guideline to support accessing material online.
* Any viewing of inappropriate or illicit material or images or downloading of such material on any computer on the school premises is strictly forbidden. In the event of accidentally accessing any of the above, the staff member will immediately turn off the computer and report the incident to the Principal / ICT Co-coordinator
* Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
* Discussion forum and newsgroups will only be used for educational purposes by school personnel.
* Face-to-face physical meetings organised via social networking sites through the school computers are strictly forbidden
* Teacher / pupils will not examine, use or change another person’s files, user name or password without the other person’s and the teacher’s permission.
* Pupils will be made familiar with copyright issues relating to online learning.
* Students will never disclose or publicise their own or another person's personal information eg home addresses, phone numbers, photographs.
* Downloading materials or images not relevant to their studies, is in direct breach of the school’s acceptable use policy.
* The school may monitor and archive all internet usage including distributing or receiving information, checking user files, temporary internet files and history . School related or personal usage may be monitored for unusual activity, security and/or network management reasons.
* As children access the senior end of the school (3rd class) they will be given a pupil's understanding (set out in Appendix 2) which is presented at a level which is commensurate with their age and understanding. These forms will be retained by the school.

Use of Email

* Students may only use approved email accounts under supervision by or with permission from the class teacher.
* Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
* Children are not allowed to access their own email accounts in school.
* Students will not reveal their own or other people’s personal details, such as addresses or telephone numbers 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 permissionfrom their teacher.
* Parents and staff should only communicate through the official school email addresses or platforms agreed within the school such as Aladdin, Class Do jo, Zoom, See-saw, Google suite.

Internet Chat

* Students will only have access to discussion forums or other electronic communication forums that have been approved by the school.
* Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
* Usernames will be used to avoid disclosure of identity.
* Arranging to meet physically with someone organised via Internet chat or any platform is strictly forbidden.

Personal Devices including Mobile Phones

Children are not permitted personal devices in school. Any child found with a mobile phone or other personal device from home is in breach of the AUP and the Code of Behaviour and will have be required to leave the device in the Principal’s office. A parent/guardian will need to call to the Principal’s office to collect his/her child’s phone. The school is indemnified from any loss or damage to children’s’ personal devices.

School Website: **www.maristprimaryschool.ie**

* Parents/Guardians indicate on the school application form if consent is given for their child’s photographs to be included on the school website. From time to time, students’ projects, artwork or school work may be published on the website.
* The publication of student work will be co-ordinated by a teacher.
* Digital photographs of individual pupils will not be published on the school website. Photographs will focus on groups rather than individuals.
* Personal pupil’s information (name, address etc) will be omitted from the school web pages.
* The school website will avoid publishing the first name and last name of individuals in a photograph.
* The school will ensure that the image files are appropriately named – will not use students’ names in image file names or ALT tags if published on the web.
* Students will continue to own the copyright on any work published.

**School social media.**

Parents are requested not to share any photos of other people’s children on any social media platform.  This includes photos which they may take themselves at school events, or photos shared by the school.

**Education and Internet Awareness**

The Marist Primary School regularly undertakes an education programme to educate children and parents on the safe, responsible use of the Internet. Cyber-bullying is a significant threat. Through education and awareness, we aim to limit our children’s susceptibility to it as they progress to secondary school. 21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time, they need to learn to recognise and avoid these risks – to become internet wise.

Resources that may be used to implement this programme include:

* Don't be mean behind the Screen
* Zeeko
* SPHE Programmes
* Webwise[www.webwise.ie](http://www.webwise.ie) Resources
* Use of the ‘Kids’ section on the [www.webwise.ie](http://www.webwise.ie) website

**Distance Learning**

We recognise that online collaboration is essential for distance learning. The Marist Primary School may help to provide access to a variety of online tools, which will assist in providing more effective teaching and learning remotely, while also enabling greater communication between staff, families and students. The same rules of conduct and behaviour will apply to distance learning as apply in the classroom and the guidelines set out in Appendix 1 should be read in conjunction with this Acceptable Use Policy

Staff

* The Internet is available for Staff personal and professional use. Personal use of the Internet should not occur during class time.
* Staff should not use their mobile phones in the vicinity of children, except for educational purposes and in emergencies.

Support Structures

* The school will inform parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.
* The school will inform parents if it is made aware of inappropriate social media use by children outside of school
* From time to time parents will receive information and advice regarding Internet safety in the home.

Sanctions

* Some material available on the Internet is unsuitable for children and therefore the guidelines in this policy must be adhered to at all times. Access to the Internet will be withdrawn from pupils who fail to maintain acceptable standards of use. Internet access in school includes a strict filtering service yet no filtering service is completely fool proof.
* Intentional/deliberate misuse of the Internet will result in disciplinary action in line with our school’s sanctions as outlined in the School’s Behaviour Policy including in extreme cases suspension or expulsion.
* Sanctions for pupils who bring a mobile phone or personal device to school or upload images in school onto personal devices are outlined in the School’s Behaviour Policy and can in extreme cases result in suspension or expulsion
* The school also reserves the right to report any illegal activities to the appropriate authorities.

**Ratification/ Implementation/Review**

The reviewed AUP was ratified by the Board on 16th September, 2020. It was communicated to parents through the school newsletter and made available to all parents throughthe school website.

**Appendix 1**

**Guidelines for good online distant learning communication in the Marist Primary School**

1. For any Video Call with a child, two members of staff will be present
2. Under no circumstances can photos, screen shots or recordings be taken of any Video Call or audio.
3. Staff, families and students are expected to behave in an appropriate, safe, respectful and kind manner online.
4. It is the duty of parents/guardians to supervise children while they are working online and to ensure any content that they are submitting to their teacher is appropriate.
5. Staff members may communicate with pupils and their families via Aladdin or through an established app or agreed platform (eg. Seesaw, Class Dojo, Zoom, Google Suite etc) or if via email through the email provided by the Parent/Guardian. Separate consents will be sought prior to a child accessing a class account on an educational platform.
6. Any electronic forms of communication will be for educational purposes and to allow for communication with families.
7. Students and staff will communicate using tools or through Video Calls (such as Zoom) which have been approved by the school and of which parents have been notified (eg Seesaw, Classdojo, Google Suite etc).
8. Parental permission will be acquired before setting up a profile for a pupil on a communication forum.
9. For Video Calls, parental permission is implied, as the link to a video call will be communicated via the parent/guardian’s email address. Essentially, by virtue of the pupil logging on to the call, permission is assumed.
10. For security reasons, passwords will be provided to families, where applicable.
11. The Marist Primary School cannot accept responsibility for the security of online platforms, in the event that they are hacked.
12. Communication using a mobile phone will not be frequent, but in the rare exception where it is necessary, staff members will ensure that their caller ID is private.

**Guidelines for staff members using online communication methods:**

1. For any Video Call with a child, two members of staff will be present
2. Under no circumstances can photos, screen shots or recordings be taken of any Video Call or audio.
3. Staff members will communicate with pupils and families during the hours of 8.50am - 2.30pm, where possible.
4. Staff members are expected to present and act in a professional manner at all times which engaging with children on a Video Call.
5. An appropriate background/setting should be chosen for the Video Call.
6. Staff members will have high expectations regarding pupil behaviour, with any communication which takes place online.
7. Staff members will seek to become familiar with Apps. before using them with pupils.
8. Staff will check that consent has been given, before setting up a pupil profile for an online app.
9. Staff members will report any concerns regarding online behaviour or interactions to School Management.
10. Staff are encouraged to generate a new meeting ID and password for each Video Call Meeting being held.
11. Staff members will notify parents/guardians of the date, time and password for a Video Call via email.
12. Staff members will only admit participants to video conferences, if they recognise the email address/username as being connected to a pupil.

**Guidelines and good practice for pupils using online communication methods:**

For submitting learning:

1. Submit work and pictures that are appropriate - have an adult take a look at your work before you send it.
2. Use kind and friendly words.

For Video Calls:

1. Under no circumstances can photos, screen shots or recordings be taken of any Video Call or audio.
2. Remember our school rules - they are still in place, even online.
3. Set up your device in a quiet space, with no distractions in the background.
4. Join the video with your microphone muted.
5. Raise your hand before speaking, just like you would do in class.
6. If you have the chance to talk, speak in your normal voice, using kind and friendly words.
7. Show respect by listening to others while they are speaking.
8. Ensure that you are dressed appropriately for the video call.
9. Be on time - set a reminder if it helps.
10. Enjoy! Don’t forget to wave hello to everyone when you join!

**Guidelines for parents and guardians:**

For learning

1. It is the responsibility of parents and guardians to ensure that pupils are supervised while they work online.
2. Check over the work which pupils send to their teacher, ensuring it is appropriate.
3. Continue to revise online safety measures with pupils.

For Video Calls

1. Under no circumstances can photos, screen shots or recordings be taken of any Video Call or audio.
2. Ensure that the school has the correct email address for inviting you to join apps and meetings.
3. The main purpose of a video call is to maintain a social connection between the school staff and pupils. Encourage pupils to listen and enjoy the experience.
4. Be aware that when participating in group video calls, you can be seen and heard unless you are muted or have disabled your camera. Accordingly, parents/guardians should be mindful about what family activities would potentially be heard/seen during the students’ use of video conferencing.
5. An appropriate background/setting should be chosen for the video call.
6. Participants in the call should be dressed appropriately.
7. You will automatically enter a waiting room when the code for a Zoom call has been entered. Please note that school staff will only accept users into video call if you can be identified by the display name on your zoom account.
8. Please ensure that your child is on time for a scheduled video, or they may be locked out. Please request to join the Zoom call approximately five minutes before the scheduled start time. This will give school staff time to verify your email address.
9. Make sure to familiarise your child with the software in advance. For video in particular, show them how to mute/unmute and turn the camera on/off.
10. For detailed information on GDPR and Zoom, please visit <https://zoom.us/privacy>

It is important to note that any breach of the above guidelines will result in a discontinuation of this method of communication. A breach may also result in a person being immediately removed from a meeting or in a meeting being immediately terminated. In this case, the child’s parent will receive a report on the incident.

**Appendix 2**

**Pupil Undertaking**

We use the School Computers and Internet Connection for learning. These rules will help us to be fair to others and keep everyone safe.

* I will ask permission before entering any website, unless my teacher has already approved that site
* I will not bring external storage devices such as pen drives (or memory sticks/USB keys etc.) into school without permission
* I will not use or change another person's file, user name or password without the other person's and the teacher's permission.
* I will not download material or images which are not directly relevant to my studies.
* I will only use emailfor school projects and with my teacher’s permission.
* The messages I send will be polite and sensible. I will never send, receive or repost any material that is illegal, obscene, hateful or defamatory or that is intended to annoy or intimidate another person
* I will not reveal my own or other people's personal details such as home addresses, phone numbers, photographs, or other personal information through the internet.
* I will never arrange a face-to-face physical meeting with someone that I have only connected with through emails or the internet
* I will ask for permission before opening an e-mail or an e-mail attachment
* If I see anything I am unhappy with or if I receive a message I do not like, I will tell a teacher immediately.
* I know that the school may check my computer files and may monitor the sites I visit.
* I understand that if I deliberately break these rules, I could be stopped from using the Internet and computers and my parents will be informed.

**Signed**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Pupil

**Signed**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Parent/Guardian

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

**Appendix 3 - Permission Form**

Parent/Guardian

As the parent or legal guardian of the above pupil, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access the Internet. I understand that 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 pupils access unsuitable websites. As the parent or legal guardian, I also agree to the Distant Learning Guidelines that form part of the Acceptable Use Policy.

I accept the above paragraph □ I do not accept the above paragraph □
*(Please tick as appropriate)*

**Parent’s Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **Parent’s Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_