St. Joseph's Primary School,
Macroom
Co. Cork
Phone 026 41847
email stjosephsmacroom@gmail.com

Acceptable Internet Usage Policy 2020-2022

The internet is a valuable teaching and learning tool. It provides information and allows people to communicate with others and share information. It can develop children's independent research skills and promote life-long learning. However, in its largely unregulated state, the internet can also present a number of risks for children and therefore these guidelines will be followed when using the internet in school. This policy should be read in conjunction with the school's ICT Policy.

Aim

The aim of this Acceptable Internet Usage Policy (AUP) is to ensure that pupils will benefit from learning opportunities offered by the school's internet resources, in a safe and effective manner.

Pupils' Use of the Internet

Pupils are responsible for their own good behaviour on the internet. Access to the internet may be withdrawn from pupils who fail to maintain acceptable standards of use. Internet access in the school is filtered to minimise the risk of exposure to inappropriate material. However, no filtering service is completely foolproof and therefore pupils will be supervised during the use of the internet.

Parents of pupils from Junior Infants to 2nd class will sign to give permission for their child to have supervised access to the internet for educational purposes. Pupils from 3rd to 6th class will co-sign this form with their parents.

Teachers will ensure, to the maximum extent possible, that pupils know and understand that no internet user is permitted to:

- ➢ Use the internet for any illegal activity including accessing other computers.
- ➢ Retrieve, send, copy or display offensive messages or pictures.
- ➢ Use obscene or offensive language.
- ➢ Cause damage to computers, computer systems or networks.
- ➢ Violate copyright laws.
- ➢ Disclose or publicise their own or another person's personal information.

- ➢ Use another user's password.
- ➢ Trespass in another user's folders, work or files.
- ➢ Cause any form of vandalism to the machine or the work of others including the uploading or creation of viruses.
- ➢ Copy or share any material distributed by the teacher without permission.
- ➢ Record the teacher in any way using photo or video.

Organisation and Management of Internet Use

Teachers will select sites which will support pupils' learning. Pupils may be given details of suitable sites to extend their learning at home as and when appropriate.

Promoting Safe and Independent Use of the Internet

Internet access will be supervised. Teachers will ensure that pupils understand appropriate use of the internet and are aware of the rules. Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable. Children will be taught lessons on internet safety to give them more knowledge on the topic. Parents/Guardians will also be informed on the possible dangers of using the internet.

Children's Use of Email, Messaging and Social Networks

Children in school are encouraged to use email for educational purposes. Pupils will not be allowed to send personal emails from the school system without permission. Incoming email will be regarded as public and may be examined by any staff member. The use of chat rooms, messaging services or social networking sites is forbidden unless with the expressed permission of the class teacher. Teachers can create student email addresses for school work only. This will be monitored by the class teacher. Teachers will create emails for students operated from within the schools Microsoft Office for Education platform.

- **Following Rules Shall Apply:**
    - ❖ Email will be used for educational purposes only.
    - ❖ Students will use an approved email account under the supervision of a teacher.
    - ❖ Pupils will not send or receive any material that is offensive, illegal or obscene, or that is intended to annoy or intimidate another person.
    - ❖ Pupils will not send messages to or from school email unless instructed to by a teacher.
    - ❖ Pupils will never arrange to meet someone via a school email.
    - ❖ Pupils will not reveal personal details via school email.

- **Use of School iPads**

    - ❖ Everything accessed on a laptop/iPad is monitored by a teacher.
    - ❖ Each device will be assigned to a specific group/student.
    - ❖ iPads are expected to remain in school at all times. However, should an iPad be brought home with a student it is at the student/parents own risk.
    - ❖ Parents should be vigilant if a school laptop/iPad is brought home.
    - ❖ Parents are responsible for the supervision of students while using a laptop/iPad at home.
    - ❖ Students are never permitted to alter settings on the devices which may cause harm or access inappropriate material.
    - ❖ Students are forbidden from recording teachers at all times.
    - ❖ Devices are only to be used under the direction of the teacher.

Inappropriate Usage

Internet use and access are considered a school resource and privilege. Therefore, if the school's AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions will be imposed in line with the school's Code of Behaviour. Such sanctions may include but are not limited to:

- Written warning

- Temporary withdrawal of access privileges.

- In extreme cases, suspension or exclusion.

The school will be obliged to report any illegal activities to the appropriate authorities.

Staff Acceptable Usage

Members of staff are encouraged to use various online resources in their teaching and learning activities, to conduct research, and for contact with others. Each member of staff has access to their own school email address as part of his/her work, protected by the use of a confidential password, which should be kept secure. The use of email for personal use is acceptable outside of teaching hours and during breaks. When using the internet, all users must comply with all copyright, libel, fraud, and discrimination and obscenity laws. Staff members should not in any way alter the filtering preferences. When setting up any school-based learning applications such as Seesaw or , teachers should always do so using official school emails. A serious breach may be treated as a disciplinary matter.

Staff members should:

- Follow the guidelines in this AUP.
- Return a signed application form stating their agreement with this policy.
- Supervise student use where possible.
- Model and provide ethical and appropriate use of technology in the classroom.
- Maintain a curricular focus.
- Ensure all students have signed AUP permission form.
- Keep student email address details safe and secure.
- If taking photos on a personal device, the teacher should then upload photos to OneDrive on Office 365 or the school's Facebook page or school website using a school account within 2 days and delete from the personal device immediately after.
- Not transfer, request or receive any materials inconsistent with the ethos of the school.
- Not contact students through school email addresses outside of educational purpose.

Teachers may use school ICT equipment outside of school hours but they do so at their own risk. Should damage or loss occur during this time, the teacher must cover the cost.

School Website and Social Media:

- Pupils may create projects, artwork, writing or audio and visual recordings which would be suitable for publication on our school website or social media platforms.
- Designated teachers will manage the publication of material on these platforms while adhering to school stipulations.
- Personal pupil information will not be published.
- Class lists, full names of pupils will not be published alongside identifying photographs.
- Digital photographs, video clips will focus on groups and group activities rather than on individuals.
- Pupils will be given the opportunity to publish such projects on all social media platforms.
- Teachers will select work to be published and decide on the appropriateness of such work.
- Permission to publish students' work will be signed in AUP permission slip. Permission may be withdrawn at any time.
- Pupils will continue to own the copyright of any work published.
- Teachers may use a range of media platforms to display digital classwork. Teachers must monitor all material.
- All staff must be sensitive about material posted on personal social media where they must ensure that both the school or students are not identified.

Remote Learning to Continue Online Teaching and Learning (During school closures)

While St. Joseph's engages in Remote/Online Learning to continue teaching and learning, all teachers should:

- Ensure they have full parental permission with each child who has been registered or is given access to a Virtual Learning Environment (VLE)
- Be available for school-related queries, either from students, parents or staff members during regular school hours of 09:00-14:40.
- Use and check their school email every day.
- Only communicate with students and parents using school-based platforms such as Microsoft Teams or VLE's such as Seesaw or Class Dojo etc.
- Never upload or post any personal information.
- Monitor student comments and posts while keeping a record of any misdemeanours.
- Ensure settings are in place online where students can't see or comment on other students' work.
- Should set up a VLE enabling teachers to assign school material and also provide feedback to students.
- Relay to parents that any breach of the school policy could result in their child being removed from the online learning environment.

With regards to online, live or pre-recorded lessons and taking into account child protection guidelines, teachers should:

- Ensure that they are using platforms which are set up using school emails and school regulated platforms (e.g. Microsoft and Google-owned platforms).
- Teachers may use video hosting software, such as Zoom, where the software is established as GDPR compliant.
    - It is compulsory that such platforms are set up using official school emails/accounts and that all students use school emails/accounts to enter and participate on the call.
- Ensure children are appropriately dressed or else remove them from the call and report it immediately to the DLP.
- Advise children to be in a non-private room (e.g. bedroom) but if they are, a door should be kept open.
- Advise parents to supervise the lesson or at least take regular check-ins with the lesson.
- Ensure that an appropriate background is used for themselves and students where a video call may be involved.
- Make sure they are in a suitable environment if making video calls.
- Relay to parents that any breach of the school policy could result in their child losing privileges of video lessons.

Success Criteria

The success of this policy will depend on the following:

i. Teachers continued use of Acceptable Internet Usage Policy as a communication tool with children and Parents/Guardians.

ii. Procedures outlined in the policy is consistently followed.

iii. Feedback from teachers/parents/pupils regarding aspects of the policy.

iv. Feedback from the inspectorate.

Implementation (a) Roles and Responsibilities

The Board of Management, the Parents/Guardians, the Principal and Class Teachers of St. Joseph's primary School, Macroom will be responsible for the successful implementation of the Acceptable Internet Usage Policy. The policy will be implemented immediately.

(a) Roles and Responsibilities

It will be necessary to review this policy on a regular basis to ensure optimum implementation of the Acceptable Internet Usage Policy in the school. Those involved in the review will include:

• *Teachers* • *Pupils*• *Parents* • *BOM* • *DES*

The policy was drafted by Digital Strategy Co-ordinator Cornelia Cronin in July 2020 and reviewed by Digital strategy team and staff in August 2020. The policy was distributed via the website to Parents/Guardians in September 2020.

(b) Timeframe

Date of review: June 2022

Ratification and Communication

This policy was ratified by the Board of Management in September 2020.

Chairperson of the Board of Management:

Principal:

Date:

Internet Usage Policy APPENDIX 1

LETTER TO PARENTS/GUARDIANS

Dear Parents/Guardians,

As part of the school's provision of Information Technology experiences, the children will have supervised access to the internet for educational purposes. An example of this usage may include: research projects, educational videos, educational games and software. Teachers will inform the students to the best of their knowledge in the use of the most appropriate websites and resources. As you are aware, the Internet contains a vast amount of information but unfortunately not all of this is suitable for children and so we have produced an Acceptable Internet Usage Policy specifying our guidelines. On occasion, your child may be asked to "Bring their Own Device" in order to facilitate the education purposes outlined above.

Before being allowed to use the Internet, all pupils must obtain parental permission. We therefore ask that both you and your child sign the detachable slip below as evidence of your approval and acceptance of the school rules on this matter. A copy of our Acceptable Internet Usage Policy is available on the school's website and hard copies are available from the school.

Please read the Acceptable Internet Usage Policy carefully.

ACCEPTABLE USE OF THE INTERNET PERMISSION SLIP

I give permission for my child(ren) to have access to the internet in school and accept school rules on this matter.

Name of Pupil(s) .....

Signature of Parent/Guardian .....

Signature of Pupil(s) ..... (3^{rd}-6^{th} class)

Acceptable Internet Usage Policy APPENDIX 2

Advice for Parents/Guardians on Internet Usage in the Home

ICT in schools is growing more important every year. We here at St.Joseph's feel that students deserve the right to learn and develop appropriate usage and skills to help them as best as possible for the future technology-filled world.

During school hours, teachers will guide pupils toward appropriate materials on the internet. Outside school, Parents/Guardians should bear the same responsibility for such guidance as they normally would with other information sources, such as television, magazines etc.

Parents/Guardians should be aware that the internet service provider at home may not be filtered. See the WebWise online collection of Internet Safety Resources website (www.webwise.ie) for advice on Cyber Bullying, Facebook and other social networking sites.

It is important that these guidelines are followed:

- Discuss rules for using the internet with your children and decide together when, how long and what is seen as appropriate use.
- Be aware of the sites your children are visiting and discuss with them what they are learning.
- Ensure that children do not give out personal identifying information on the internet such as a picture, full name, home address, email address, phone number, school name or financial information such as credit card or bank details.
- Encourage your children not to respond to any unwelcome, unpleasant or abusive messages and to inform you if they receive any such messages or images.
- Reinforce with your child that if they do not know someone personally they should not be communicating with them online.
- Ensure privacy settings for all messaging and social networking services are adequately set to prevent children from giving out detailed personal and/or location information.
- Appropriate home use of the internet can be educationally beneficial and can make a useful contribution to home and school work. It should, however, be supervised and Parents/Guardians be aware that they are responsible for their children's use of the internet resources at home.