

Scoil Réalta na Maidine

Internet Acceptable Use Policy

Introduction

Scoil Réalta na Maidine recognizes that access to Information and Communication Technology (ICT) gives our students enhanced opportunities to learn, engage, communicate and develop skills. To that end, we provide access to ICT for student use. The aim of this Internet Acceptable Use Policy (AUP) is to ensure that children will benefit from learning opportunities offered by the school's ICT resources in a safe and effective manner.

This version of the AUP was revised by the principal and staff in consultation with the Board of Management and parents in October 2020. NCTE guidelines were followed re same. It will be assumed that parents/guardians accept the terms of the AUP unless the school is otherwise specifically notified.

The Board of Management reserves the right to amend this policy to adapt to changing circumstances entirely at its discretion.

Purpose

This Acceptable Use Policy (AUP) outlines the guidelines, behaviours and minimum standards that our students are expected to follow when using current and future school technologies. Students are expected to follow the same rules for good behaviour and respectful conduct online as offline. This policy should therefore be read in conjunction with the Scoil Réalta na Maidine Code of Behaviour and Anti-Bullying Policy where these rules are found. 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 Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions, as outlined in the AUP, will be imposed.

Scope

This Policy applies to staff and students of Scoil Réalta na Maidine. This Policy has been drawn up to protect our students from the risks associated with the Internet while they are at school and it applies to all of the school's "Devices", which means all computers, iPads, laptops, smart phones and other IT resources that connect to the school's network. Parents/Guardians are advised however that while the children may be given internet based homework assignments from time to time, the school takes no responsibility for the internet usage of the students while they are outside the school. It is important that parents/guardians monitor their own child's internet usage at home and ensure that their children are aware and respectful of the risks involved.

This Policy should be read carefully to ensure that the content is accepted and understood.

School's Strategy

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:

General

- Internet sessions will always be supervised by a teacher or computer tutor.
- The centrally managed content filtering service provided by the School's Broadband Network will be used in order to minimize the risk of exposure to inappropriate material.
- The school will regularly monitor pupils' Internet usage through classroom observation.
- Students and teachers will be provided with training 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 personal memory sticks, CD-ROMs or other digital storage media in school requires a teacher's or tutor's permission.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
- Websites will be previewed/evaluated by a teacher using a filtering system, before being integrated into lessons conducted on school devices.
- It is important to note that as per the school's Code of Behaviour and Anti-Bullying Policy parents/guardians and students should be aware that placing a once-off, offensive or hurtful internet 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 will be regarded as bullying behaviour.

World Wide Web (Use of the Internet)

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials and the school will not be responsible for any attempts taken in this regard.
- Students will report accidental accessing of inappropriate materials in accordance with school procedures.

- In the event of accidentally accessing any of the above sites, the student will be expected to immediately turn off the monitor and report the incident to a teacher or supervisor.
- Students will use the Internet for educational purposes only.
- All websites used by the teachers to enhance learning will be vetted in advance by the teacher.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Students will not upload, download or otherwise transmit material that is copyrighted on school devices.
- 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.
- Students will be taught specific lessons on online safety by teachers.
- Students will not examine, change or use another person's files, username or passwords. The school takes every reasonable precaution to provide for online safety, but it cannot be held responsible if students access unsuitable websites either deliberately or inadvertently.

Email

- Students will use approved class email accounts under supervision by or permission from a teacher or computer tutor or parent/guardian.
- 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 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 permission from their teacher or computer tutor.

Internet Chat

- Students will only have access to chat rooms, discussion forums, messaging 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 identify.
- Face-to-face meetings with someone organised via Internet chat will be forbidden.

Distance Learning

- In circumstances where teaching cannot be conducted on the school premises, teachers and S.N.A.s acting under the direction of teachers, may use a range of online platforms such as Google Classroom, Google Meet and SeeSaw to assist with remote/distance teaching and learning where necessary.
- The school will sign up to the terms of service of the Online Platforms in use by the school.
- The School will enable the most up to date security and privacy features which these Online Platforms provide.
- Staff members will adhere to school guidelines on the use of platforms for live engagement.
- Parents will be asked to sign a consent form for their children to engage with teachers and SNAs using online platforms.
- In the case of Google Classroom and Google Meet, parents/guardians must grant access to their child to have a school Gmail address such as pupilname.student@school name.ie
- Parents/guardians will be provided with the password and will be expected to monitor their child's use of the Gmail address and Online Platforms.
- If teachers or SNAs are using Google Meet, parents/guardians must consent to their child having a school email address as above to allow their child access to the lessons or meetings. Where the child does not have a school email address, parents can consent by submitting their own email address for their child to access meetings or lessons on Google Meet.
- Parents/guardians must also agree to monitor their child's participation in any such lessons conducted on the Online Platform and to be in the room with the child for any one-to-one meetings or classes.

School Facebook and Website

- The facebook page and website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The facebook page and website will be checked frequently to ensure that it does not contain personal details.
- The publication of student work, displays will be co-ordinated by a teacher or tutor.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Visual content focusing on individual students will not be published on the school facebook and website.
- Personal pupil information including home address and contact details will be omitted from facebook page and website.
- The school facebook will avoid publishing the first name and last name of individuals in a photograph or in relation to any individual work displayed.
- The school will ensure that the image files are appropriately named – will not use pupils' names in image file names or ALT tags if published on the web.
- Pupils will continue to own the copyright on any work published.

Personal Devices

The use of mobile phones is strictly forbidden.

- Pupils using their own technology in school, such as having in their possession a mobile phone or smart watch, turning it on or using it in class, sending nuisance text messages, or taking of images with a mobile phone camera, still or moving is in direct breach of the school's acceptable use policy.
- Students may not use any personal device with recording or image taking capability while in school or on a school outing. Any such breach of the Acceptable Use Policy (AUP) will be sanctioned accordingly.
- Any images or recordings taken by class teachers on smartphones or other personal devices must be downloaded onto the school server and/or on to the school App/relevant school affiliated website and then immediately deleted from source.
- The use of E-readers may be permitted, under the supervision of the teacher. All personal devices are to be turned off during school hours.

Critical Incident and Social Media Use

Scoil Réalta na Maidine recognises that social media is now part of everyday communication and information sharing. In the event of a Critical Incident, the school community (staff, children and other relevant community members) are asked to respect the privacy and sensitivities of individuals or families involved by carefully considering whether indeed they should post any comments on social media. The school also reminds parents/guardians to discuss social media use with their children and advise that its use is monitored more actively following a crisis.

Legislation

The school will provide information on the following legislation relating to use of the Internet with which teachers, students and parents should familiarise themselves.

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988
- Children First 2018
- EU General Data Protection Regulations 2018
- Anti-Bullying Guidelines for Primary Schools 2013

Support Structures

- The school will inform students and parents of key support structures and organization that deal with illegal material or harmful use of the Internet.
- The school will regularly run a programme on acceptable internet usage, for students and parents/guardians. This will cover several topics including cyber.bullying.
- Staff will regularly partake in Continuous Professional Development in relation to the development of AUPs, internet safety and cyber-bullying.

Use of Information Communication Technology (“ICT”) Resources

Scoil Réalta na Maidine’s information and technology resources (e.g. e-mail, computers, computer applications, networks, internet, intranet, facsimile, phone and other wireless communications devices, telephone, paging and voice mail systems and the like) are school property and are provided solely for school related activities.

Inappropriate use including hacking, pirating software, using school resources for non-school commercial activities, soliciting, distributing literature for outside entities, disclosing confidential information of the school, sending inappropriate e-mail or accessing inappropriate web sites (such as those advocating hate or violence, containing sexually explicit material promoting illegal activities), or using school resources in a way that violates the letter or spirit of the school’s policies or reflects negatively on the school is forbidden.

Users of the school’s information and technology resources must not share passwords. If you allow others to use your password or assigned resource, you will be held responsible for their use.

Consistent with national laws, the Board of Management reserves the right to monitor the use of its information and technology resources and to take appropriate disciplinary actions, or denying future access privileges in cases of misuse. Staff/student use of the school’s information and technology resources constitutes consent to such monitoring. All such monitoring will be conducted in accordance with law including, where applicable, the EU’s General Data Protection Regulation (“GDPR”).

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion in line with the Code of Behaviour.

The school also reserves the right to report any illegal activities to the appropriate authorities.

Access to the Internet will be withdrawn from students who fail to maintain acceptable standards of use.

Roles and Responsibilities

The Board of Management is responsible for the formulation of this policy.

The principal and staff are responsible for the implementation of this policy during the school day.

Parents/Guardians are responsible for the internet usage of the students while they are outside school.

Review

This policy and its associated procedures will be monitored on an ongoing basis and it is envisaged that the school, BOM and parent representatives will revise the AUP regularly and as necessary.

Implementation and Communication

This policy will be implemented from the date of ratification. Parents/guardians will be made aware of the policy on enrolment. The policy will be available to view on the website or on request through the school office.

This policy has been ratified by the Board of Management.

Signed: _____
Chairperson

Date: _____