Acceptable Use Policy Guidelines

Guidelines for developing an Acceptable Use Policy in school

PDST Professional Development Service for Teachers | An tSeirbhís um Fhorbairt Ghairmiúil do Mhúinteoirí

Co-financed by the Connecting Europe Facility of the European Union

An Roinn Oideachais Department of Education

Introduction

Devising an Acceptable Use Policy (AUP) is an important first step in addressing the issue of digital safety at school level. The following information provides guidelines and advice on the issues involved in this process.

Developing an Acceptable Use Policy

Components of an Acceptance Use Policy

Useful Templates

Developing an Acceptable Use Policy (AUP)

An Acceptable Use Policy is a document which addresses all rights, privileges, responsibilities and sanctions associated with the use of the internet and digital technologies within the school, including online and offline usage. It is usually drawn up by teachers and school leadership as part of a consultative process and often incorporated into the school's overall Digital Learning Plan. Students should also be included in the consultation process in an age-appropriate manner. Ideally, every school will devise an AUP before it is involved in any use of the Internet and will seek Board of Management ratification (for legal reasons).

Included in this publication is a sample AUP for teachers. In general, it addresses the safe, acceptable and responsible use of the internet and digital technologies. It may be used as a framework or customised to reflect individual school circumstances and needs. (This publication also includes guidelines on the use of different aspects of the Internet. These can be adapted or subsumed into the AUP provided, should the school opt to include that level of detail).

As the rationale for having an AUP is primarily to promote good practice and safe, responsible use of the internet and digital technologies, it is a very important document. Its main goals are:

- To educate students, parents and teachers about the potential of the internet and digital technologies as a valuable learning resource
- To identify the school strategy on promoting the safe use of the Internet and address the risks associated with its use
- To provide schools with legal protection from liability

Explaining to students why an AUP exists and how it operates may sound obvious, but it is still an important step in raising awareness and providing students with understanding into various digital technology and Internet safety issues. Whilst regulation and technical solutions are very important, their use should be balanced by educating students to take a responsible approach. The education of students is an essential part of the school's digital learning plan. Children and young people need the help and support of the school to recognise and avoid safety risks and build their resilience. A planned internet safety programme should be provided as part of SPHE/Wellbeing or other curriculum areas and should be regularly revisited with key safety messages reinforced as part of a planned programme. Online safety and digital wellbeing resources and advice is available from webwise.ie; the online safety initiative of the Department of Education.

Components of an AUP

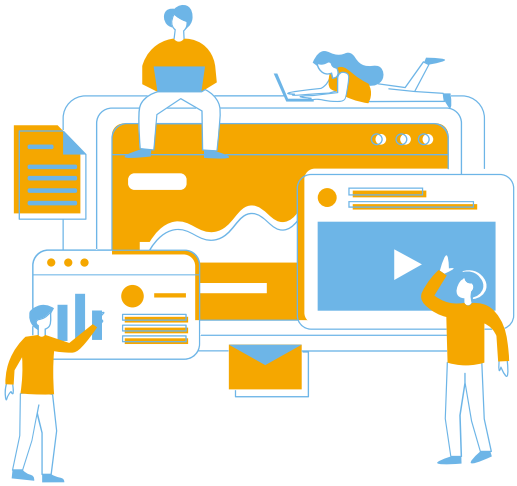
An AUP should address all aspects of usage of digital technologies and the internet. These include, but are not limited to:

Section 1: Online

- Broadband filtering level
- Searching, downloading and browsing websites
- Copyright guidelines
- Publishing a school website
- Online communication such as email, social media, online forums, messaging etc.
- Online gaming

Section 2: Platforms

- Digital learning platforms
- Use of email accounts
- Capturing and storing media
- GDPR



Section 3: Internet Safety

- Where to locate online safety advice and guidelines
- Definition of inappropriate material
- Illegal and harmful use of the Internet
- Use of equipment for commercial gain
- Use of email accounts
- Sanctions
- Reporting mechanisms

webwise.ie

Suggested steps to follow in developing and updating this policy:

1 - Initiate and establish structures
Establish a co-ordinating group/ sub-group of the digital learning team, if considered necessary

2 - Review and Research
Reference the key information on the webwise.ie and gov.ie/en/organisation/department-of-education/websites which provide information, advice, and tools to support schools in being proactive in the area of internet safety and are designed to be adaptable to the needs of individual schools

3 - Preparation of draft policy
Share the following template materials below:
Sample Acceptable Use Policy (AUP) – template format
Permission slip for signature by parent/guardian – appended to template
Letter to Parents/Guardians
AUP Checklist

Amend the AUP to suit the needs of the school - each school's own context will influence the approach adopted

4 - Circulation/ Consultation
Circulate the draft policy and consult with school staff, students, parents/guardians, board of management/trustees
Amend the draft policy, as necessary, in light of the consultation process

5 - Ratification and Communication
Present the policy to the Board of Management for ratification
Make provision for the circulation of the policy to all parents/guardians and arrange to provide it to all students, including new entrants
Communicate the ratified policy to other members of the school community

6 - Implementation
Implement the provisions of the policy

7 - Monitoring
Check, at regular intervals, that the policy is being implemented and identify any issues arising

8- Review, Evaluation and Revision
Review and evaluate the impact of the policy in line with the digital learning plan regularly, and at least annually (AUP checklist will assist this process) in light of the evaluation process, feedback from school community and other developments

Acceptable Use Policy Template

School Name: _____

Address: _____

_____

The aim of this Acceptable Use Policy is to ensure that students will benefit from learning opportunities offered by the school's digital resources in a safe and effective manner. The responsible use of internet and digital technologies, both online and offline and access is considered an integral part of teaching and learning. Therefore, if the school AUP is not adhered to agreed sanctions will be imposed.

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

This version of the AUP was created/updated on _____ (date) and ratified on _____ (date).

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

- 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 should 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 external digital storage media in school, requires a teacher's permission
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute

Internet Use

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials
- Students will be encouraged to report accidental accessing of inappropriate materials in accordance with school procedures
- Students will use the Internet 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 or passwords
- Downloading by students of 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 of the internet and school's digital platform, including distributing or receiving information, school-related or personal, will be monitored

Email

- Students will use approved school email accounts
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy, harass 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
- Students will not forward email messages or screenshots of emails or "reply all" without the permission of the originator
- Students must only use their school email for school related activities and for registering on school based activities only. The use of personal email addresses is not allowed for school based work
- Students should not use school email accounts to register for online services, social networking, apps or games
- Students should 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 report any such communications to a teacher
- Students should avoid opening emails that appear suspicious. Students should report any suspicious emails to a teacher
- All emails and opinions expressed in email are the responsibility of the author and do not reflect the opinion of the school

Social Media and messaging services for Staff and Students

- All members of the school community must not use social media, messaging services and the internet in any way to harass, impersonate, insult, abuse or defame others
- Staff and students must not discuss personal information about students, staff and other members of the school community on social media
- Staff and students must not use school email addresses for setting up personal social media accounts or to communicate through such media
- Staff and students must not engage in activities involving social media which might bring the school into disrepute
- Staff and students must not represent their personal views as those of the school on any social media service or message services
- Students will be provided with guidance on etiquette regarding social media

Schools can also direct staff to Guidance for Registered Teachers about the use of Social Media and Electronic Communication.

Guidance for Teachers

Schools may also direct staff to Guidance for Registered Teachers about the use of Social Media and Electronic Communication here:

- https://www.teachingcouncil.ie/en/news-events/latest-news/2021/guidance-for-registered-teachers-about-the-use-of-social-media-and-electronic-communication.html

Digital Learning Platforms (including video conferencing)

- The school's digital learning platform is owned and managed by the school. This platform should enable two-way communication
- Prior acceptance from parents should be sought for student usage of the schools' digital learning platform
- Use of email accounts (as noted above)
- Only school devices should be used for the purposes of capturing and storing media.
- All school-related media and data should be stored on the school's platform
- The use of digital platforms should be used in line with considerations set out in the school's data protection plan (GDPR)
- Each user of the platform should have their own unique login credentials. Personal email addresses should not be used when creating accounts on school digital platforms
- Passwords for digital platforms and accounts should not be shared

Remote Learning
Please use this space to detail information on the school Remote Learning Policy

Images & Video

- Care should be taken when taking photographic or video images that students are not identifiable (no names mentioned etc)
- Care should be taken when taking photographic or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Students and staff must not take, use, share, publish or distribute images of others without their permission
- Taking photos or videos on school grounds or when participating in school activities is only allowed with expressed permission from staff
- Students and staff must not take or share images, videos or other content online with the intention to harm another member of the school community regardless of whether this happens in school or outside
- Sharing explicit images and in particular explicit images of students and/or minors is an unacceptable, illegal and absolutely prohibited behaviour, with serious consequences and sanctions for those involved. Sharing explicit images of other students automatically incurs suspension as a sanction and will be reported to the appropriate authorities

Communications

This is an area of rapidly evolving technologies and uses. Schools will need to discuss and agree how they intend to implement and use new and old technologies. For example, some schools do not allow students to use personal devices (smartphone/tablet/smartwatch etc.) in lessons, while others recognise their educational potential and allow their use.

A wide range of rapidly developing communications technologies has the potential to enhance learning. There is a table included below to shows how a school might consider the benefit and risks/disadvantages of using these technologies for education. This section may also be influenced by the age of the students. The table has been left blank for your school to choose its own responses.

Communication Technologies	Allowed	Allowed at certain times	Allowed with staff permission	Not Allowed
Personal Devices may be brought to school				
Use of personal devices in lessons				
Use of personal devices in social time				
Taking photos on personal devices (smartphone, tablet, etc.)				
Use of hand-held devices				
Use of personal email addresses in school, or on school network				
Use of school email for personal emails				
Use of chat rooms				
Use of instant messaging				
Use of social media sites and online forums				
Use of blogs				

The school may also wish to add some policy statements about the use of communications technologies in place of, or in addition to the above table.

Inappropriate Activities

The following list should help identify "inappropriate activities" in your school. You should add ticks to the relevant columns and then include the appropriate statements in the AUP policy.

Users should not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: (Tick all that apply)

- ◯ Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer
- ◯ Misuse and fraud legislation
- ◯ Racist material
- ◯ Pornography
- ◯ Promotion of any kind of discrimination
- ◯ Promotion of racial or religious hatred
- ◯ Harmful content or threatening behaviour, including promotion of physical violence or mental harm
- ◯ Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- ◯ Using school systems to run a private business
- ◯ Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- ◯ Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- ◯ Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords
- ◯ Creating or propagating computer viruses or other harmful files
- ◯ Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- ◯ Online gaming
- ◯ Online gambling
- ◯ Online shopping
- ◯ Use of social networking sites, instant messaging and online forums
- ◯ Child sexual abuse material
- ◯ Any other activity considered questionable

School Website

- Students will be given the opportunity to publish projects, artwork or school work on the internet in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website
- The website will be regularly checked to ensure that there is no content that compromises the safety of students or staff
- Website using facilities such as comments and user-generated content will be checked frequently to ensure that they do not contain personal details
- The publication of student work will be coordinated by a teacher
- The school will endeavor to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will only be published on the school website with parental permission
- Personal student information including home address and contact details will be omitted from 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 and will not use students' names in image file names or ALT tags if published online
- Students will continue to own the copyright on any work published

Cyberbullying

Bullying is *'unwanted negative behaviour, verbal, psychological or physical, conducted by an individual or group against another person (or persons) which is repeated over time'*. (Anti-Bullying Procedures, Department of Education, 2013)

This definition also includes:

- deliberate exclusion, malicious gossip and other forms of relational bullying
- identity-based bullying such as homophobic bullying, racist bullying, bullying based on a person's membership of the Traveller community and bullying of those with disabilities or special educational needs
- cyberbullying

Cyberbullying is the use of technology to bully a person with the intent to hurt, humiliate or intimidate them. Cyberbullying can take many forms including exclusion online, hurtful messages/images, abusive messages/emails, imitating someone online, etc. This type of bullying is increasingly common and is continuously evolving.

Department of Education Anti-Bullying Procedure, 2013 defines cyberbullying as "placing a once-off offensive or hurtful public message, image or statement on a social network site or another public forum where that message, image or statement can be viewed and/or repeated by other people will be regarded as bullying behaviour"

As cyberbullying uses technology to perpetrate bullying behaviour and does not require face to face contact, cyber-bullying can occur at any time (day or night). Many forms of bullying can be facilitated through cyber-bullying. For example, a target may be sent homophobic text messages or pictures may be posted with negative comments about a person's sexuality, appearance etc.

Access to technology means that cyberbullying can happen around the clock and the students' home may not even be a safe haven from such bullying. Students are increasingly communicating in ways that are often unknown to adults and free from supervision. The nature of these technologies means digital content can be shared and seen by a very wide audience almost instantly and is almost impossible to delete permanently. While cyberbullying often takes place at home and at night, the impact can also be felt in school.

In accordance with the Anti-Bullying Procedures for Schools; 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 **will be regarded as bullying behaviour.**

When using the internet 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.

Measures are taken to ensure that staff and students are aware that bullying is defined as unwanted negative behaviour, verbal, psychological or physical, conducted by an individual or group against another person (or persons) and which is repeated over time. This definition includes cyberbullying even when it happens outside the school or at night.

Personal Devices
Students using their own technology in school should follow the rules set out in this agreement. They will only use personal devices (smartphone, tablet, smartwatch etc.) in school under the direction and/or supervision of a teacher if they have permission.

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

- Data Protection Acts 1988 to 2018 and General Data Protection Regulations (GDPR)
- Copyright and Related Rights Act 2000
- Child Trafficking and Pornography Act 1998 and Criminal Law (Sexual Offences) Act 2017
- Children First Act 2015
- Harassment, Harmful Communications and Related Offences Act 2020 (Coco’s Law)
- Criminal Damage Act 1991

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.

Sanctions

Misuse of the Internet and digital technologies will result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities, including An Garda Síochána. These sanctions are laid out in the Code of Behaviour and Anti-Bullying Policy.

Sample Permission Form Template

Please review the attached school Acceptable Use Policy, and sign and return this permission form to the Principal/Year Head/Class Tutor.

School Name: _____

Name of Student: _____

Class/Year: _____

Student
I agree to follow the school's Acceptable Use Policy on the use of the internet and digital technologies. I will use the internet and digital technologies in a responsible way and obey all the procedures outlined in the policy.

Student's Signature: _____ Date:

Parent/Guardian
As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and 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 students access unsuitable websites.

In relation to the school website, I accept that, if the school considers it appropriate, my child's school work may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing students' work on the school website.

Signature: _____ Date: _____

Address: _____

_____

_____

_____

Telephone: _____

Sample Letter to Parents/Guardians

Dear Parent/Guardian,

Re: Safe and Responsible Use of the Internet

As part of the school's education programme we offer students supervised access to the Internet. This allows students access to a large array of online educational resources that we believe can greatly enhance the learning experience.

However, access to and use of the Internet and digital technologies requires responsibility on the part of the user and the school. These responsibilities are outlined in the school's Acceptable Use Policy (enclosed). It is important that this enclosed document is read carefully, signed by a parent or guardian and returned to the school.

Although the school takes active steps to promote safe use of the Internet, it recognises the possibility that students may accidentally or deliberately access inappropriate or objectionable material.

Having read the terms of our school's Acceptable Use Policy, you may like to take a moment to consider how the Internet is used in your own home, and see if there is any way you could make it safer for your own family.

Parents/Guardians can find a range of advice, support, tools and resources on the Webwise Parents Hub available on **webwise.ie/parents**. On the hub you'll find explainer guides to popular apps, talking points, how to guides, expert advice videos and a free Parents' Guide to a Better Internet.

Yours sincerely,