



Coole NS

Acceptable Use Policy

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 Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed. Coole NS also encourages its children to view Internet and other computer use as both an additional learning tool and recreational activity where appropriate.

This Policy applies to all of the school's devices, which means all computers, laptops, smart phones and other IT resources that connect to the school's network. This Policy applies to staff and students of Coole NS. The School reserves the right to amend this policy from time to time entirely at its discretion. This Policy should be read carefully to ensure that the content is accepted and understood. The aim of the Acceptable Use Policy is to ensure that students benefit from the learning opportunities offered by internet access in a safe and positive manner. This Policy also aims to establish minimum standards for, and let the students, parents/guardians know of the school's administration and monitoring of, the schools' devices, equipment and networks.

School

The School employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies include, but are not limited to the following:

A firewall is used on school Devices to minimise the risk of exposure to inappropriate material and to block unsuitable sites. This is regularly updated.

Students and teachers will be provided with training by teachers in the area of research techniques specific to the Internet. Online safety training will be provided to teachers and will be taught to all students.

Uploading and downloading of non-approved software on school devices will not be permitted.

Virus protection software is used on school devices and updated regularly.

A teacher will always supervise Internet sessions which are conducted on school Devices.

Websites will be previewed / evaluated by a teacher using a filtering system, before being integrated into lessons conducted on school Devices.

The School's search engine has a built in 'safe search' feature. The 'safe search' feature will be enabled on all search engines on school Devices.

It is important to note that the school's Anti-Bullying Policy should be read in conjunction with this 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.

Use of the Internet

Students will not knowingly attempt to visit Internet sites on school Devices that contain obscene, illegal, hateful or otherwise objectionable materials and the school will not be responsible for any attempts taken in this regard. 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.

The internet will be used to enhance learning and will be used for educational purposes. All websites used by the teacher will be vetted in advance by the teacher.

Students will not disclose or publicise personal or confidential information to others online.

Examples of this are, but not limited to, their own or classmates' home addresses, telephone numbers, email addresses, online profile information or name and location of their school. Students will not examine, change or use another person's files, username or passwords.

Students will be aware that any usage, including distributing or receiving any information, school-related or personal, may be monitored for unusual activity, security, and/or network management reasons. 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.

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 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.

Distance Learning

In circumstances where teaching cannot be conducted on the school premises, teachers may use Zoom, SeeSaw, Aladdin Connect or other platforms approved by the Principal as platforms to assist with remote teaching where necessary.

Zoom is a video-conferencing platform which will enable teachers, staff and pupils to connect via a live link. Teachers will connect with pupils using pre-arranged Zoom Meetings. Rules for pupils using online communication methods:

1. Remember to ensure you join each Zoom meeting using your family name.
2. Pictures or recordings of the video call are not allowed.
3. Remember our school rules - they are still in place, even online.
4. Set up your device in a quiet space, with no distractions in the background.
5. Join the video with your microphone muted.

6. Raise your hand before speaking, just like you would do in class.
7. If you have the chance to talk, speak in your normal voice, using kind and friendly words.
8. Show respect by listening to others while they are speaking.
9. Ensure that you are dressed appropriately for the video call.
10. Be on time - set a reminder if it helps.
11. Enjoy! Don't forget to wave hello to everyone when you join!

Guidelines for parents and guardians:

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/Zoom

1. Under no circumstances should pictures or recordings be taken of video calls.
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 engage in online learning activities while maintaining a social connection between the school staff and pupils.
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.
5. 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. (i.e. Family Name)
6. 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.
7. 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.
8. Participants in the call should be dressed appropriately.
9. An appropriate background/room should be chosen for the video call.
10. For detailed information on GDPR and Zoom, please visit <https://zoom.us/privacy>

Internet Chat

Discussion forums on Online Platforms will only be used for educational purposes and will always be supervised.

School Website and affiliated Applications.

The school's website address is <http://coolens.ie/>

- The School uses the Aladdin App.
- Students will be given the opportunity to have photos, projects, artwork and other work relating to curricular and extra-curricular school activities published on the school website as per the consent form. Teachers will coordinate the publication of this material. Personal information relating to the student including their name, home address and contact details will not be included on school social media or the school's website. Digital photographs and audio or video clips of individual students will not be published on the school website

and/or affiliated pages, without prior parental/guardian permission. Instead, photographs etc. will focus on group activities, where children will not be named. Photos/Videos may be used for the production of the Homework Journal or specific school events e.g. Communion etc. These photos/videos and the photos/videos on our website/App should not be copied or posted to any social media or other website or published in any way. Parent(s)/guardian(s) are requested not to 'tag' photographs or any other content which would identify any children or staff in the school.

Parent(s)/guardian(s) are requested to ensure that online messages and/or comments to the school's social media sites are respectful.

- The Principal will review the content of the website regularly. The Principal and the Board welcome any suggestions about how the content may be improved.
- If any parent or guardian has any concern about the appropriateness of the content of the website or social media sites, then the Board asks that the matter be brought to the attention of the Principal as a matter of urgency.
- This Policy should be read in conjunction with our Data Protection Policy.

Personal Devices

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. All personal devices are to be turned off during school hours.

Legislation and Regulation

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

EU General Data Protection Regulations 2018

Anti-Bullying Guidelines for Primary Schools 2013

Data Protection (Amendment) Act 2003

Child Trafficking and Pornography Act 1998

Video Recording Act 1989

The Data Protection Act 1988

Interception Act 1963

Use of ICT Resources

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 or any activity which is in contravention with this Policy, may result in disciplinary action, including written warnings, withdrawal of access privileges, and, where appropriate, 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.

Dear Parent(s)/Guardian(s),

The staff and Board of Management of school name have recently reviewed the school's Acceptable Use Policy (A.U.P). Please familiarise yourself with this policy, prior to completing the A.U.P Permission Slip. School files will be updated accordingly and this form will be kept on file for no longer than is necessary.

Acceptable Use Policy Permission Slip

Name of student: _____

Class: _____

Parent/Guardian,

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my child to access the Internet. I understand that students may not be able to participate fully in lessons involving PCs, laptops and other IT equipment without consenting to our Acceptable Use Policy.

Parent/Guardian Signature: _____ Date: _____