

CBS Primary School,

Chapel Street,

Dundalk,

Co. Louth.

A91 YF82

Telephone number: 042 9327861

office@cbsprimarydundalk.ie



CBS Dundalk Acceptable Use Policy

Policy Statement

CBS Primary, Dundalk is committed to providing pupils with the best opportunities to access internet resources in the context of their individual and overall learning whilst protecting the rights and confidentiality of all persons in the school.

Policy Purpose

This policy aims to provide school staff, parents, and pupils with guidance on the safe and acceptable use of the internet and electronic devices in school.

We aim to ensure that pupils will benefit from the school's internet resources' learning opportunities safely and effectively.

Internet use and access are considered a school resource and privilege. Therefore, if the school AUP has not been adhered to, this privilege will be withdrawn, and appropriate sanctions will be imposed.

Policy Scope

This policy applies to all staff, parents, pupils, visitors, and other persons engaged in school activities.

General Principles

The school employs several strategies to maximise learning opportunities and reduce risks associated with the internet;

The school will ensure where practicable that a teacher supervises internet sessions.

Students may not have internet access unless a prior agreement is made with the teacher and the teacher is present.

Filtering software and equivalent systems are used to minimise the risk of exposure to inappropriate material.

Uploading and downloading of non-approved software is not permitted.

Virus protection software is used and updated regularly.

The use of personal memory sticks or other digital storage media in school requires a teacher's permission.

Students must always treat others with respect while online and not undertake any actions that may bring the school or themselves into disrepute.

World Wide Web

- Students must use the internet for educational purposes only.
- Students must not intentionally visit Internet sites that contain obscene, illegal, hateful, or otherwise objectionable materials.
- Students must report accidental access to inappropriate materials to their class teacher, who may refer the matter to the principal.
- Students must not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Students must never disclose or publicise personal information.
- Downloading materials or images not relevant to their studies directly breach the school's acceptable use policy.
- Students are informed that any usage, including distributing or receiving information, school-related or personal, will be monitored for unusual activity, security, or network management reasons.

Email / Internet Chat

- Students must only use approved class email accounts under supervision by or permission from a teacher.
- Students must not send or receive any illegal, obscene, and defamatory material intended to annoy or intimidate another person.
- Students must not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Students must never arrange a face-to-face meeting with someone they only know through emails or the internet.
- Students must note that sending and receiving email attachments/files are subject to permission from their teacher.
- Parents and staff should communicate through the official school email address or school email addresses provided by teachers, rather than teachers' personal email addresses.
- Students may send homework/work to email accounts created by their teachers.
- The school currently uses Seesaw and Clasdojo learning apps for remote learning; parental permission will be sought.
- Students only have access to chat rooms, discussion forums, messaging, or other electronic communication that the school has approved.
- Chat rooms, discussion forums and other electronic communication forums must only be used for educational purposes.
- Usernames are used to avoid disclosure of identity.

School Website

Pupils will be allowed to publish projects, artwork or schoolwork on the World Wide Web following clear policies and approval processes regarding the content that can be loaded to the school's website. A teacher will coordinate all such publication.

- The website is regularly checked to ensure that no content compromises the safety of pupils or staff.
- A teacher will manage the publication of student work.
- Personal pupil information, including home address and contact details, will be omitted from school web pages.
- The school's website will avoid publishing the first name and last name of pupils in a photograph.
- The school will ensure that the image files are appropriately named and 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.

Internet

The internet has become a two-way communication system for the school and the wider community. The school uses services such as Facebook, Twitter, and other social media to communicate with parents. Although not owned by CBS Primary, Dundalk, these services form part of our web services and all content that is placed on these services fall under this policy.

Our children's safety on the web is of utmost importance, so the following rules apply to the school and parents.

The internet is open to potential dangers when used inappropriately.

The school asks:

- While the school will not monitor this, we would advise parents not to allow their children to have personal accounts on Facebook, Twitter, etc., until they are the appropriate age. Many social media sites have minimum age requirements.
- Please do not "tag" photographs or any content to identify any child or staff member in the school.
- Please ensure that online messages and comments to the school are respectful. Any messages written on social media are treated in the same way as written messages to the school.
- Avoid any negative conversations about children, staff, or parents on social media accounts. If you have an issue with something in the school, social media is not the place to raise it. Comments of this nature will be deleted.
- Please do not request to "friend" a member of staff in the school. Staff would like to keep their personal lives personal. It may be awkward for a staff member to be asked to ignore a Facebook or other social network request.
- Please do not add advertisements to our social media account without the prior permission of the principal.
- Failure to keep the above rules will result in a permanent ban on our social media account.

Photographs

Photographs of the children will only be displayed online through our various platforms with explicit consent from parents/guardians on enrolment.

Online Learning Platforms/Remote Learning

Since March 2020, online learning platforms have become a vital part of teaching and learning in the CBS Primary School.

We have been using "Seesaw" for Remote Learning. (Seesaw is GDPR compliant)

Please refer to our **Remote Teaching and Learning policy** for further detailed guidelines. It is published on our school website.

The following guidelines apply when using Seesaw:

- Parental consent is required before use.
- Home Learning codes are given to students to sign in; these codes remain active for a year.
- Teachers will send class announcements and activities which pupils and parents can see.
- Students post work and assignments in their journals.
- Parents can view their children's journal and posts.
- Students do not see the work of other students in the class.
- Teachers control who can see messages or access a student's journal content by authorising specific people to connect to that student's account, e.g., School Principal, SEN Teacher/SNA

- Teachers may also choose to publish some class content to a public class web page managed by Seesaw.

Direct communication using the internet:

Teachers in the school may choose to use several classroom communications tools, such as Seesaw, Zoom and Google Meets (please refer to our Remote Teaching and Learning Policy for more details). Zoom and Google Meets provides synchronous video opportunities whereby a staff member directly speaks to the children live. The staff member invites pupils and their families to these meetings using a code. The following are ground rules for synchronous lessons online.

- All meetings will be password protected.
- All people involved in the meeting will conduct themselves in a similar manner that would be expected in a regular class.
- The child must be sitting in a communal room, i.e., Sitting room or kitchen. Under no circumstances should a child be in a bedroom for live interactions.
- The child must be dressed appropriately.
- The teacher will mute all mics for the group; the teacher controls who speaks.
- The child will enter the meeting using their own name.
- A child may consider changing their background for privacy; this is available on some devices. An appropriate background /picture should be chosen.
- The teacher will organise a timetable for live interactions.
- Under no circumstances can live interactions be recorded. This is in breach of child protection and GDPR guidelines.
- If a child turns off their camera, the teacher will request that it is turned back on; if the child continues to have the camera off, they will be automatically removed from the meeting.
- If a child engages in inappropriate behaviour, the teacher will request that the child refrains from this behaviour; if the child refuses, the teacher will remove the child from the meeting. The principal will be contacted immediately.
- For a 1:1 live lesson (SET), a parent must sit with the child during the lesson.
- For all other groupings, the parent must be present in the room during the interaction.

Personal Devices /Mobile phones

- Pupils are not permitted to bring mobile phones or any other electronic devices to school. In an exceptional circumstance, a prior agreement must be made with the Board of Management. This decision will be made on a case-by-case basis. A parent must apply in writing stating the reasons why an exemption should be made. The principal may make a temporary agreement and issue a letter granting temporary permission until the next Board of Management meeting. Under these exceptional circumstances, mobile phones will be kept in the office or kept with the class teacher.
- Children who need to contact home during school hours may do so through the school secretary using the school landline phone.
- Pupils who ignore this policy and use a personal device on school premises without permission will be required to hand over their device to a staff member, and parents will be asked to collect it from the school office. The phone will be inspected to ensure that no content identifying another pupil or staff member is stored and any relevant material will be deleted immediately by the child with an adult present.
- Pupils who ignore this policy and are involved in activities such as leaving a device turned on or using it in class, sending nuisance text messages, or the unauthorised taking of images with a recording device, still or moving, is in direct breach of this policy.
- The Board of Management accepts no responsibility for replacing lost, stolen, or damaged personal devices, nor does it accept responsibility for loss or damage sustained while travelling to and from school.

- Pupils using personal devices to bully other pupils or send offensive messages will face disciplinary actions as per the School Code of Behaviour and the Anti- Bullying Policy.
- Where it is suspected that a pupil has made an inappropriate recording on a personal device, the teacher may request the pupil to hand over their device and seek to view the recording. Where necessary, the teacher may ask a parent to be present when viewing this material. Where there is a suspicion that the device's material may provide evidence relating to a criminal offence, the device will be handed over to the Gardai, with the parents' knowledge, for further investigation.
- It should be noted that it is a criminal offence to use an electronic device to menace, harass or offend another person. If action, as sanctioned by the school in this regard, is deemed ineffective, as with all such incidents, the Board of Management may consider it appropriate to involve the Gardai.

Sanctions

Misuse of electronic devices will result in disciplinary action, including written warnings, withdrawal of access to privileges and, in some cases, suspension or expulsion (see Anti Bullying Policy). The school also reserves the right to report any illegal activities to the appropriate authorities.

Cyber Bullying

Cyber Bullying is the use of ICT (usually a mobile phone or the internet) to abuse another person. It can take place anywhere and can involve many people. Anybody can be targeted, including pupils, school staff, and members of the wider school community. It can include threats, intimidation, harassment, cyber-stalking, slander, defamation, exclusion, peer rejection, impersonation, and unauthorised publication of private information or images. There are many types of Cyberbullying.

The more common types are:

- Text messages - can be threatening or cause discomfort.
- Picture/video clips via mobile phone cameras/devices – images sent to others to make the victim feel threatened or embarrassed.
- Mobile phone calls – silent calls, abusive messages.
- Emails – threatening or bullying emails, often sent using a pseudonym or somebody else's name.
- Chat room bullying – menacing or upsetting responses to children or young people when in a web-based chat forum.
- Bullying via websites – use of defamatory blogs (web logs), personal websites, gaming websites, and online personal 'own web space' sites such as YouTube, Facebook, Twitter, Snapchat, and Myspace, among others.

Procedures for preventing Cyberbullying:

- Staff, pupils, parents, and the Board of Management are made aware of cyberbullying issues.
- Pupils and parents will be urged to report all incidents of cyberbullying to the school. All reports of cyberbullying will be noted and investigated according to the school's Anti-Bullying, Mobile Phone, Child Protection, and Behaviour Policies, where applicable.
- Staff CDP (Continuous Professional Development) will assist in keeping up to date with current technologies.
- Pupils will learn about cyberbullying through Social, Personal and Health Education (SPHE), Assemblies, Friendship Week activities and other curriculum projects.
- Pupils, parents, and staff will be involved in reviewing and revising this policy regularly.

Legislation

CBS Primary School provides information to staff and parents on relevant legislation relating to the use of the internet, including:

- Child trafficking and Pornography Act 1998

- Video Recordings Act 1998
- The Data Protection Acts 1988-2018

Support Structures

The school will inform students and parents of key support structures and organisations that provide support and advice on illegal material or harmful use of the Internet, e.g.

- <https://zeeko.ie/>
- <https://www.webwise.ie/>
- [https://www.safefood.eu/Education/Primary-\(ROI\)/MediaWise.aspx](https://www.safefood.eu/Education/Primary-(ROI)/MediaWise.aspx)
- <https://www.common sense media.org/>
- <https://cybersafeireland.org/>
- <https://www.gov.ie/en/campaigns/be-safe-online/>
- <https://kidshealth.org/en/parents/net-safety.html>
- <http://www schooldays.ie/articles/5-internet-safety-steps-parents-should-take>
- <http://www.justice.ie/en/JELR/Pages/Cybercrime>

AUP for Staff and Visitors

Staff and Visitors

- The school's computer system is provided and managed by the school. It is made available to staff to further their professional development and the education of the students in the school.
- Access to the school's computer facilities is a privilege and not a right.
- Any staff member or visitor who abuses this privilege will be immediately excluded from accessing and using the computing facilities.
- Exclusion from using the school's computer will prevent the user from recovering files and using the facilities.
- The Board of Management may change this policy to include changes in the law or the acceptable practice of internet use and reserves the right to make such changes without notice and whenever required.
- All users are responsible for ensuring that they have read and understood the current policy.
- This policy is published on our school website; therefore, acceptance of the AUP policy is assumed once using its system and accounts. It is a requirement of CBS Primary, Dundalk, that all users of its network or facilities accept and adhere to the school's Acceptable Use Policy.
- The Board of Management reserves the right to examine or delete any files that may be held on its computer network, to monitor websites visited and online activity, and to view any email messages passing through or saved on the system.

Inappropriate Activities

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals, or comments that contain or relate to:

- **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
- Threatening behaviour, including the promotion of physical violence or mental harm
- Any other information that may be offensive or breaches the integrity of the school's ethos or brings the school into disrepute.
- Use systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by the school revealing or publicising confidential or proprietary information (e.g., 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) causes network congestion and hinders others from using the internet.
- Online gaming (except for educational pre-approved online games found on our ICT Internet Resources folder)
- Online gambling, shopping/commerce
- Use of social networking sites.
- The user agrees to refrain from sending or receiving any material, which may violate copyright (including intellectual property rights), confidence, privacy, or other rights. If you are in any doubt as to the legality of what you are doing or propose to do, you should either seek independent legal advice or cease that usage.
- Sharing or making references to a student's work, particularly if it could undermine the student, is not accepted.

- Users should be aware that the storage, distribution of, or transmission of illegal materials may lead to investigation and possible prosecution by the authorities.
- Users may not gain or attempt to gain unauthorised access to any computer for any purpose. In addition to being in breach of this AUP, such action may lead to criminal prosecution under the Computer Misuse Act.
- Users must not send data via the internet using forged addresses or data which is deliberately designed to adversely affect remote machines (including but not limited to denial of service, ping storm, Trojans, worms, and viruses).
- Users must not send unsolicited commercial or bulk email, commonly referred to as 'spam' or 'UCE.'
- Users are prohibited from running 'port scanning' or other software intended to probe, scan, test vulnerability of, or access remote systems or networks except in circumstances where the remote user has given express permission for this to be done.
- Users may not divulge their computer network passwords to third parties and must take all reasonable steps to ensure that such information remains confidential.
- In the event of a teacher's absence, the school principal will furnish a substitute teacher with login details to the class computer and password for Databiz.
- All substitute teachers will adhere to this AUP Policy.
- Activity that threatens the school's ICT systems' integrity or activity attacking or corrupting other systems is forbidden. Such activity includes browsing system files and changing any system settings.
- Personal USB storage devices should be monitored for corruption and used with caution. If a USB storage device presents signs of corruption or potential virus activity, it must no longer be used within the school's computer network.
- Use of the computing facilities for personal financial gain, gambling, political purposes, or advertising is forbidden.

(*These activities are illegal in Ireland)

Minimising risk when using Social Media:

Acknowledging that there is a range of experience among teachers regarding their use of electronic communication and social media, the following is a reminder as to how staff members may minimise risk when using social media and electronic communication:

- Teaching staff must adhere to the Teaching Council Code of Professional Conduct and Social Media Guidelines.
- All staff members must adhere to school policies, procedures, and guidelines in relation to social media use.
- The staff member's responsibility is to familiarise themselves with any social media application before using it and be clear about its advantages/disadvantages.
- All staff must conduct themselves appropriately online not to undermine the school's image or reputation.
- Always maintain professional boundaries with students.
- Never exchange personal phone numbers, personal email addresses or photographs of a personal nature with students or parents.
- Never accept or initiate Facebook friend requests, or other such invites, with current students or parents.
- Discretion should be used when dealing with friend requests from former students or parents of former students.
- Review your privacy settings regularly to minimise risks.
- Consider your settings on social media sites. You may wish to prohibit others from tagging you in any photograph or update without your permission.

- Be aware of photographs published online, which include you, and where they may be posted.
- Do not discuss students, parents, or colleagues online.
- Protect yourself by constantly logging out of any social media site you are using at the end of a session.

Unacceptable uses of Social Media sites

- Sending or posting discriminatory, harassing, negative comments, threatening messages or images that may cause harm to any member of the school community.
- Forwarding or 'Liking' material likely to cause offence or hurt to any school community member.
- Sending or posting messages or material that could damage the school's image or reputation.
- Creating a fake profile that impersonates another member of the school community.
- Sending or posting material that is confidential to the school.
- Participating in the viewing or exchange of inappropriate images or obscene material.

Whilst every attempt has been made to cover a range of situations, it is recognised that this policy cannot cover all eventualities. All cases involving the inappropriate use of social media will be dealt with on an individual basis by the Board of Management. Disciplinary action will be taken in the case of inappropriate use of social media tools.

Legislation

CBS Primary, Dundalk provides information to staff and parents on relevant legislation relating to the use of the internet, including:

- Child trafficking and Pornography Act 1998
- Video Recordings Act 1998
- The Data Protection Acts 1988-2018

The Board of Management adopted this policy.

Chairperson signature: _____

Date: _____

Date of the next review: April 2023

CBS Primary School,

Chapel Street,

Dundalk,

Co. Louth.

A91 YF82

Telephone number: 042 9327861

office@cbsprimarydundalk.ie



Acceptable Use Policy Permission Form

Parent/Guardian:

As the pupil's parent or legal guardian, I have read the Acceptable Use Policy and grant permission for my child to access the internet.

I understand that Internet access is intended for educational purposes.

I also understand that the school has taken every reasonable precaution to provide for online safety, but the school cannot be held responsible if pupils access unsuitable websites.

I accept the above paragraph **I do not accept the above paragraph**

(Please tick as appropriate)

In relation to the school website and school social media accounts, I accept that my child's schoolwork, photographs or videos may be chosen for inclusion on the website and social media accounts if the school considers it appropriate.

I understand and accept the terms of the Acceptable Use Policy relating to the school website and social media account.

I accept the above paragraph **I do not accept the above paragraph**

(Please tick as appropriate)

Signature: _____ Date: _____

CBS Primary School,

Chapel Street,

Dundalk,

Co. Louth.

A91 YF82

Telephone number: 042 9327861

office@cbsprimarydundalk.ie



GDPR compliance

Dear Parents and Guardians,

To ensure our school is compliant with GDPR (General Data Protection Regulations), please complete the following: I give consent for:

(Child's Name:) _____

Photographs and videos to be taken of my child for in-school displays, for publication on the school website and social media accounts.

Photographs of my child to be taken for publication in local & national newspapers/magazines.

Our school photographer will take class/group photographs.

These photographs are a lovely keepsake, and often the teacher/principal may distribute photographs containing more than one child to individual children in the class.

This consent will be held on file for the duration of your child's education here at CBS.
Consent may be withdrawn at any time in writing to the Principal/Data Controller

Signed: _____ Date: _____

CBS Primary School,

Chapel Street,

Dundalk,

Co. Louth.

A91 YF82

Telephone number: 042 9327861

office@cbsprimarydundalk.ie



Internet Safety Acceptable Use Policy (AUP)

AUP User Agreement

As a school user of the network and internet at CBS Dundalk, I have read and understood the Acceptable Use Policy (AUP) for the use of the internet, and by signing it, I agree to abide by the policy as stated and to accept any sanctions which may be imposed due to misuse of the internet and non-adherence to the AUP.

I agree to follow the school rules on its use. I will responsibly use the network and observe all the restrictions explained in the AUP. I agree to report any misuse of the network to the school Principal or the Board of Management.

If I do not follow the rules, I understand that this may result in loss of access to the internet/computer network as well as other disciplinary action.

Name: _____

Signature: _____

Date: _____