Acceptable Use Policy

San Carlo Senior National School,

Leixlip, Co. Kildare

General Approach –

The aim of this Acceptable Use Policy (AUP) 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 as outlined in this AUP.

This policy applies to all devices i.e. all computers, iPads, laptops, smart phones, smart watches and other technology resources. This Policy applies to staff and students of Scoil San Carlo S.N.S.

It is important to note that the school's Code of Behaviour and Bí Cineáltas 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.

It is envisaged that the school will revise the AUP every 2 years (or sooner in the light of issues that may arise). The AUP is available on the school website and should be read carefully to ensure that the conditions of use are understood and accepted.

The 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 –

1. Filtering software controlled by the NCTE will be used in order to minimise the risk of exposure to inappropriate material.
2. Internet use within school will always be supervised by a teacher.
3. Students and teachers are provided with training in the area of internet safety.
4. Uploading and downloading of non-approved software will not be permitted.
5. Websites will be previewed / evaluated by a teacher **before** being integrated into lessons conducted on school devices.
6. Virus protection software will be used and updated on a regular basis.
7. The use of personal external digital storage media in school requires a teacher's permission.
8. Student iPads will be monitored using 'Classroom' app on the teacher iPad.
9. Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.

Internet Use –

- Pupils will **not** visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- 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 the teacher or supervisor.
- Pupils will use the internet for educational purposes only.
- Pupils will be familiar with copyright issues relating to online learning.
- Pupils will never disclose or publicise personal information, either their own or that of others.
- Students will not change or use another person's files, username or passwords.
- Students will be aware that any usage of the internet and the school's digital platform, including distributing or receiving information, school-related or personal, will be monitored.
- 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 –

- Pupils will use approved class email accounts under supervision by a teacher.
- Pupils will not send or receive any material that is illegal, obscene or defamatory or that is intended to annoy, harass or intimidate another person.
- Pupils will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Pupils will never arrange a face-to-face meeting with someone they only know through emails or the internet.

- Pupils will note that sending and receiving email attachments is subject to permission from their teacher.
- Pupils will not forward email messages or screenshots of emails or 'reply all' without the permission of the originator.
- Pupils must only use their class email for school related activities in class and for registering on school based activities only e.g. Adobe Spark/ Spark Post.
- The use of personal email addresses is not allowed for school based work, unless the teacher grants permission such as in the case of children with a report recommending assistive technology where Google Drive will be utilised under parental guidance.
- Students should not use school email accounts to register for online services, social networking, apps or games.
- Students should avoid opening emails that appear suspicious.
- Students should report 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.
- Staff will be made aware of: Guidance for Registered Teachers about the use of Social Media and Electronic Communication. 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 in 'Email').
- Only school devices should be used for the purposes of capturing and storing media accept for staff usage as outlined below (see 'Images and Videos').
- 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 –

- In circumstances where teaching cannot be conducted on the school premises, teachers may use Zoom, Padlet, Seesaw, email or other platforms such as Google Drive, agreed by the staff and approved by the Board of Management to assist with remote teaching where necessary.
- The school has signed up to the terms of service of the Online Platforms in use by the school.
- The School has enabled the most up to date security and privacy features which these Online Platforms provide.
- If teachers are using Zoom, for individual conversations with pupils, the call will only be made to the parent/guardian's device. The parent/guardian is required to be present throughout the conversations. Such conversations must not be recorded by any participant.
- Parents/guardians must also agree to monitor their child's participation in any such lessons conducted on the Online Platforms.
- Each class will have access to Seesaw using Home Learning Codes.

Images and Video –

- 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 website and then immediately deleted from source.
- Care should be taken when taking photographic or video images that students are:
    1. Not identifiable (no specific names mentioned etc.)
    2. 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.
- 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 –

- 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 AUP will be sanctioned accordingly.
- All personal devices must be turned off by pupils while on the school grounds.
- The use of e-readers may be permitted, under the supervision of the teacher.
- Students will not have access to chat rooms, discussion forums or other electronic communication forums except for educational purposes as approved by the class or learning support teacher.
- Photos can be taken using the iPads for educational purposes only.
- Personal emails can be used under parental supervision for access to Google Drive for homework purposes for children in need of assistive technology (See above 'Email'.
- 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:
    - 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
    - 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 have projects, artwork or school work published 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.
- 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.
- Students will continue to own the copyright on any work published.

Cyber-Bullying –

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'. (Bí Cineálta Procedures, Department of Education, 2024)

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.
- Cyber bullying.

In accordance with the Bí Cineálta 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.

Personal Devices –

Students may not use any personal device with recording or image taking capability at any time, while in school, on school grounds or on a school outing. Any such breach of the AUP will be sanctioned in accordance with the school Code of Behaviour. All personal devices must be turned off by pupils while on the school grounds.

Legislation –

The following legislation relates to use of the Internet which teachers, pupils and parents should familiarise themselves with

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988
- E.U. General Data Protection Regulations 2018

Support Structures –

When necessary, the school will inform pupils and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions -

- Misuse of devices may result in disciplinary action, including written warnings and withdrawal of access privileges in accordance with the school Code of Behaviour.
- 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 the Bí Cineálta Policy.

This version of the Acceptable Use Policy was revised in March 2025 and ratified by the Board of Management on March 3rd 2025.

_____

Tony Boland

Chairperson B.O.M.

_____

Cian Forde

School Principal