



Acceptable ICT Usage Policy (AUP)

St. Paul's Community College, Waterford.

St. Paul's Community College is a state school run by the Education Training Board of Ireland (ETBI). Our school is run under the ethos of the ETB and the core values underpinning its characteristic spirit. St Paul's is a state, co-educational, multid denominational school underpinned by the core values of the Ethos of excellence in Education, Care, Equality, Community and Respect.

Contents

1. Introduction	2
2. General Principles	3
3. Acceptable Use Examples	4
4. Unacceptable Use.....	5
5. Internet Safety.....	6
6. Data Protection and Privacy	7
7. School Websites and Social media	7
8. Legislation	8
Support Structures	8
Sanctions.....	9
Ratification	9
Appendix 1:.....	10

1. Introduction

Purpose and Rationale

At St. Paul's Community College, we are dedicated to providing excellence in education, in alignment with our school's ethos. To ensure inclusivity and equal opportunities for all students, we offer a variety of facilities for use by both staff and students. These include five rooms equipped with over 20 computers each, a DCG suite with 24 computers, a laptop trolley with 24 devices, departmental tablets, SEN laptops, and devices for assistive technology. These resources are available for booking where applicable, and it is imperative that students use them respectfully and responsibly.

The Acceptable Usage Policy (AUP) at St Paul's Community College aims to foster a safe, respectful, and productive digital environment for all students and staff. This policy is essential to guide the responsible use of technology and the internet. It ensures that all users understand their roles and responsibilities in maintaining a secure and respectful online space. By outlining acceptable and unacceptable behaviours, the AUP helps protect students from online risks such as cyberbullying, exposure to inappropriate content, and privacy breaches. Additionally, it supports the school's commitment to legal and regulatory compliance, including adherence to data protection laws.

Ultimately, the AUP is designed to promote digital literacy, encourage positive online interactions, and safeguard the well-being of the entire school community. 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, in line with the school's Code of Behaviour.

The school's ICT network is provided by the patron Waterford and Wexford Education and Training Board (WWETB) therefore use of these resources must be following WWETB policies and procedures. It is envisaged that school and parent representatives will review the AUP at least annually. Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

Office 365 Apps:

This is a collection of services that allows teachers and students to collaborate and share schoolwork. Every staff member and student in the school has their own

Office365 account. This allows for 1TB of cloud storage, access to the office programs online, school E-mail, and the facility to download the full version of the latest Microsoft office products onto up to five personal devices. Each student is assigned an Office 365 account accessed using a school email address and password.

The E-mail address is in the format YYFirstnameLastname@stpaulscc.ie. It is envisaged that this account will be used by students when engaging in school work or collaborating with teachers/students in the course of school work. As this account can be accessed through a web browser, students will have access both in school and at home. The school does not accept responsibility for students' use of Office 365 outside of school time. Pupils are responsible for having their login details available during school hours. Pupils should report any account issues – locked out, no access – to their class teacher. Parents are requested to monitor the student's use of the account outside of school. Sharing of school password is a breach of this AUP as detailed below and sanctions following the schools code of behaviour may be imposed.

2. General Principles

When using the internet students, parents and staff are expected:

- **To treat others with respect at all times.**
- **Not undertake any actions that may bring the school into disrepute.**
- **Respect the right to privacy of all other members of the school community.**
- **Respect copyright and acknowledge creators when using online content and resources.**

Respect for Others

All users are expected to treat each other with respect and kindness, both online and offline. This includes refraining from any form of cyberbullying, harassment, or discriminatory behaviour. Respectful communication and interactions are essential to maintaining a positive and inclusive school environment.

Privacy and Confidentiality

Users must respect the privacy and confidentiality of others. This means not sharing personal information, such as addresses, phone numbers, or passwords, without permission. It also involves being mindful of the privacy settings on social media and other online platforms to protect personal data.

Compliance with School Rules and Policies

All technology use must comply with the school's existing rules and policies. This includes adhering to guidelines on the appropriate use of school devices, internet access, and digital resources. Users are expected to follow the AUP and any other relevant policies to ensure a safe and productive learning environment.

3. Acceptable Use Examples

School Devices

- **Educational Purposes:** Using school computers, tablets, and other devices for completing assignments, conducting research, and participating in online learning activities.
- **Software and Applications:** Accessing and using educational software and applications provided by the school to enhance learning.

Online Behaviour

- **Respectful Communication:** Engaging in respectful and constructive communication with peers and teachers through email, forums, and other online platforms.
- **Collaborative Projects:** Participating in group projects and discussions using digital tools, while respecting the contributions of all members.

Personal Devices

- **School Guidelines:** Students will place their powered off personal devices in the provided magnetic pouch for the duration of the school day. These devices are not permitted to be out of the pouches on school grounds. Failure to comply with these rules will result in the sanctions outlined in the school's code of behaviour. Please see the Mobile Phone policy for further information.
- Students who experience a short-term injury whereby they are unable to write may bring a device from home with the agreement of the relevant year head. The school is not under any obligation to provide a device in these circumstances

School Devices/ Laptops

Students should only use the computers/laptops in the building when directed and supervised by a class teacher

- Laptops are only to be used by students when directed and supervised by a class teacher
- Students should only access websites for research purposes, students should not

access any website that is deemed inappropriate

- Students who do access an inappropriate website accidentally should notify their class teacher immediately
- If there is a problem logging on to a computer/laptop the student should let the class teacher know immediately
- If the computer/laptop does not work for any reason it must be brought to the attention of the class teacher immediately.
- If a student breaks (intentional or accidental) a school computer/laptop, it will be addressed in accordance with St Pauls Community College Code of Behaviour policy
- Students are not to download anything onto a school computer or laptop unless directed by the class teacher
- Unless specifically told to do so, students should not save any of their work onto the computer/laptop. All work to be saved to students OneDrive/ Teams.

Personal Devices

Students using their own technology in school, authorised by school

management, should follow the rules set out in this agreement, in the same way as if they were using school equipment.

4. Unacceptable Use

Prohibited Activities

- **Cyberbullying:** Engaging in any form of cyberbullying, harassment, or intimidation of others online.
- **Inappropriate Content:** Accessing, sharing, or downloading content that is inappropriate, offensive, or harmful (e.g., pornography, violent material).
- **Unauthorized Access:** Attempting to gain unauthorized access to school systems, networks, or other users' accounts.

Misuse of School Devices

- **Non-Educational Use:** Using school devices for non-educational purposes, such as playing games, streaming videos, or social media unrelated to school activities.
- **Tampering:** Modifying or tampering with school hardware or software settings without permission.

Personal Devices

- **Disruption:** Using personal devices in a manner that disrupts the learning environment (e.g., texting during class, playing games).
- **Unauthorized Recording:** Recording or photographing others with or without their consent, especially in sensitive areas like classrooms or restrooms.

Breach of Privacy

- **Sharing Personal Information:** Sharing personal information of oneself or others without consent, including addresses, phone numbers, and passwords.
- **Invasion of Privacy:** Accessing or attempting to access private files, emails, or accounts of others without authorization.

Plagiarism and Copyright Breach

- **Plagiarism:** Copying and pasting information from the internet or using AI-generated content without proper attribution. This undermines academic integrity and the learning process.
- **Cheating:** Using ICT tools to find answers during exams or assignments, such as searching for solutions online or using AI to generate responses.

5. Internet Safety

Strategies for Safe Internet Use

- **Strong Passwords:** Encourage the use of strong, unique passwords for all online accounts and regularly update them.
- **Secure Connections:** Advise students to use secure, encrypted connections (e.g., HTTPS) when browsing the internet.
- **Personal Information:** Teach students to avoid sharing personal information online, such as addresses, phone numbers, and passwords.
- **Phishing Awareness:** Educate students on recognizing phishing emails and suspicious links, and to avoid clicking on them.

Education on Recognizing and Reporting Online Risks

- **Workshops and Seminars:** Organize regular workshops and seminars on internet safety, covering topics like cyberbullying, online predators, and digital footprints.
- **Interactive Lessons:** Incorporate interactive lessons and activities that teach students how to identify and respond to online risks.

- **Reporting Mechanisms:** Establish clear procedures for reporting inappropriate content or online behaviour, including who to contact and how to report incidents.

Role of Parents/Guardians in Supporting Internet Safety

- **Parental Controls:** Encourage parents/guardians to use parental control software to monitor and restrict their children's online activities.
- **Open Communication:** Promote open communication between parents/guardians and children about their online experiences and any concerns they may have.
- **Educational Resources:** Provide parents/guardians with resources and information on internet safety to help them guide and support their children.
- **Modelling Behaviour:** Encourage parents/guardians to model safe and responsible online behaviour for their children to follow.

6. Data Protection and Privacy

Data Protection and Privacy Compliance

At St. Pauls Community College, we are committed to safeguarding the personal data of our students, staff, and community. We handle personal data with the utmost care, ensuring it is collected, stored, and processed securely. Our measures to protect privacy include implementing robust encryption protocols, access controls, and regular cybersecurity audits to prevent unauthorized access and data breaches in line with WWETB practices. We also educate our staff and students on best practices for data privacy and security. In compliance with data protection laws such as the General Data Protection Regulation (GDPR), we ensure that all personal data is processed lawfully, transparently, and for legitimate purposes. We have clear policies in place for data retention and disposal, and we regularly review and update our practices to stay aligned with legal requirements and education standards.

7. School Websites and Social media

- 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

- Students will continue to own the copyright on any work published
- The website will be regularly checked to ensure that there is no content that compromises the safety, privacy, or reputation of students or staff
- Webpages/Social Media platforms allowing comments or user-generated content will be pre-moderated and checked frequently to ensure that they do not contain any inappropriate or offensive content
- St. Paul's CC will use digital photographs, audio or video clips of focusing on group activities.
- The publication of student work will be coordinated by a teacher
- Personal student information including home address and contact details will not be published on St. Pauls CC webpages and/or social media

8. Legislation

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

[Data Protection Acts 1988 to 2018](#)

[General Data Protection Regulation \(EU\) 2016/679](#)

[Copyright and Related Rights Act 2000 \(as amended\)](#)

[Child Trafficking and Pornography Act 1998 to 2004](#)

[Criminal Law \(Sexual Offences and Human Trafficking\) Act 2024](#)

[Children First Act 2015](#)

[Harassment, Harmful Communications and Related Offences Act 2020 \(Coco's Law\)](#)

[Criminal Damage Act 1991](#)

[Irish Human Rights and Equality Commission Act 2014](#)

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.

Support	Where to find it
Webwise parents hub	<u>www.webwise.ie</u>

The Irish safer internet centre	https://www.ispcc.ie/tag/irish-safer-internet-centre/
NPC National Parents Council	Helpline@npc.ie Helpline: 018874477
Be Safe Online	Gov.ie/en/campaigns/be-safe-online

Sanctions

Misuse of the Internet and digital technologies should be referred to in the school's Code of Behaviour and Anti-Bullying Policy and related sanctions regarding misuse as appropriate should be outlined therein. The school also reserves the right to report any illegal activities to the appropriate authorities, including An Garda Siochana and Tusla.

Ratification

Signed: _____ Date: _____

(Chairperson of Board of Management)

Signed: _____ Date: _____

(Principal)

Appendix 1:

(Intended for student journal)

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: _____

Parent/Guardian : _____

Date: _____

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 schoolwork 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:** _____