



St Paul's Secondary School

Care - Inclusion - Respect

# ACCEPTABLE USE POLICY

Ratified: 14 October 2021

To be reviewed: November 2023

## Rationale

The aim of this Internet Acceptable Use Policy (AUP) is to ensure that pupils will benefit from the learning opportunities offered by the school's internet resources, including the school's learning platform MS Teams, in a safe and effective manner.

Internet use and access is considered a school resource and privilege and should, in no way, incur unauthorised expenses for the school. If the school AUP is not adhered to this privilege may be withdrawn and appropriate sanctions will be imposed.

This Standard applies to the following persons:

- *All employees of the School (regardless of employment status)*
- *All students of the school*
- *Independent contractors, distribution channels and their respective employees*
- *Third parties who are contracted to provide services to the School.*

1. School Technology must not be used for inappropriate purposes. Inappropriate use of technology includes but is not limited to:

- *Fraudulent or illegal purposes;*
- *Gambling or betting.*
- *Destroying, altering, dismantling, disfiguring, or disabling School Information and systems without authorization.*
- *Impersonating someone.*
- *Faking, altering, or "spoofing" messages, attachments or email; Distributing any political messages.*
- *Transmitting, downloading, storing, forwarding, sending, copying, circulating, creating, viewing, accessing, clicking-on, or browsing any materials or communications of any sites or links that are profane, hostile (i.e., bullying) or violent, obscene, pornographic, or sexually explicit.*
- *Visiting or participating in or on any social media sites and/or forwarding, downloading, or using any non-business multimedia for any of the above-noted inappropriate purposes or any other activity that may tend to bring the School into disrepute or may affect its reputation adversely.*

2. Respect intellectual property rights:

The School respects intellectual property law and will not tolerate any copyright violations of its own intellectual property rights or those of a third party, including but not limited to:

- *Downloading, storing, transporting, or copying illegal and/or unlicensed data, music, or video files.*
- *Making unauthorized copies of proprietary software or offering unauthorized copies of proprietary software to others.*

When using the internet or the school's learning platform MS Teams, pupils, 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.

- This Acceptable Use Policy applies to pupils who have access to and are users of the internet in St. Paul's Secondary School or the school's learning platform MS Teams.
- It also applies to members of staff, volunteers, parents, carers, and others who access the internet in St. Paul's Secondary School.
- Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.
- St. Paul's Secondary School will deal with incidents that take place outside the school that impact on the wellbeing of pupils or staff under this policy and associated codes of behaviour and anti-bullying policies. In such cases St. Paul's Secondary School will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school and impose the appropriate sanctions.
- St. Paul's Secondary School implements the following strategies on promoting safer use of the internet:
  - Pupils will be provided with education in the area of internet safety as part of our implementation of the Wellbeing Programme at Junior Cycle and SPHE curriculum at Senior Cycle
  - Internet safety advice and support opportunities are provided to pupils in St. Paul's Secondary School through our Induction, Pastoral Care, ICT and Peer Mentoring programmes.
  - Teachers will be provided with continuing professional development opportunities in the area of internet safety.
  - St. Paul's Secondary School participates in Safer Internet Day activities to promote safer more effective use of the internet.

This policy and its implementation will be reviewed regularly by the Board of Management.

This policy is being developed by a working group including Principal, Deputy Principal, teachers, pupils, parents/guardians, and representatives of the Board of Management.

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Surveys and/or questionnaires of pupils.
- Surveys and/or questionnaires of pupils, parents, and teaching staff.
- Should serious online safety incidents take place, the Principal will be informed.
- The implementation of this Internet Acceptable Use policy will be monitored by the Principal and Board of Management.

Mobile phones and other digital devices have the potential to interrupt class learning and to violate the right to privacy of others.

While St. Paul's Secondary School accepts that a student may have a phone /personal electronic equipment, the following policy aims to maintain a safe, nurturing, learning environment where the personal dignity and rights of all the members of the school community are preserved.

The School will NOT accept responsibility for phones / digital devices that are lost, stolen or damaged on school premises or during school organised activities on or off school grounds.

Students participating in school related activities (e.g., co-curricular, extra-curricular activities, school trips, tours etc.) must abide by the policies governing these activities as outlined and interpreted by the teacher(s) in charge.

Inappropriate use of phones / digital device to harass an individual will be dealt with in line with the School Learning Code.

### **Definition of items covered by this policy:**

Personal electronic equipment means: all phones, mp3/4 players, tablets, and all other digital devices which could be used to communicate with, record or film another individual. This policy also covers personal music equipment and any other device which could interfere with health and safety regulations, and could compromise the learning environment in St. Paul's Secondary School

### **Context of Policy:**

#### **1. Security of the learning environment in our school**

During school hours, students must give teaching and learning their full attention and participate fully in all class activities. Personal devices are only to be used in class situations whereby they are deemed to enhance teaching and learning and are permitted to be used by the teacher.

#### **2. Protection of individual persons working or studying in the school**

It is absolutely prohibited to photograph/film/record another person without his/her prior permission and approval or that of the teacher. Any phones /personal electronic equipment or any other recording devices, if confiscated, may be checked by the School authorities to ensure that they have not been misused in this manner. If it is found that a person has filmed/recorded another individual without his/her knowledge or approval, and/or if that material has been shared with other people either from one device to another or on the internet, the case will immediately be brought before the Board of Management. The most severe sanctions possible may be sought by the Board.

Circulating, publishing, or distributing (including on the internet) material associated with School activities including but not limited to material in relation to staff and students where such circulation undermines, humiliates, or causes damage to another person, is considered a serious breach of the school rules, and will result in sanctions. As part of such disciplinary action the Board of Management reserves the right to suspend or expel a student or students where it considers the student's actions warrant such sanctions.

### **3. Health and Safety Regulations**

Students must be able to hear safety instructions when issued on the school grounds and/or in the corridors and classrooms-therefore the use of personal electronic equipment is not permitted on the school grounds or in the school building during school hours unless it is for the purposes of teaching and learning. Any parent(s)/Guardian(s) wishing to urgently contact their son/daughter may contact the School Front Office to relay urgent messages. Any student needing urgently to contact their parents(s) guardian(s) may come to the school office to use the phone with their Year Head/Tutors permission.

#### **Mobile Phones:**

Confiscated phones are to be handed into the School Front Office. Confiscated phones will be returned at the end of the school day.

Any student found or reported to be using the camera of their mobile phone at any time, will have their phone confiscated and be referred to the relevant Year-Head for sanction.

#### **Parent contacting students.**

If parents need to contact their daughter during the school day, they should do so only through the School Office.

#### **Procedure when a personal mobile phone or digital device is used inappropriately**

Photos /videos may not be taken at any time in School, without the express permission of the teacher.

Students in contravention of this policy will have their phone, including sim card and battery, confiscated by a teacher.

In the event of a mobile phone being confiscated, the School will inform the Parent/Guardian of the situation.

It is the responsibility of the teacher who confiscates the phone to place it in an envelope with the student's name and class group and give it to the Year-Head or Front Office for safe keeping. The confiscation details will be recorded by the Year-Head or Secretary.

If a student refuses to hand up the phone and this refusal is accompanied by aggressive or abusive behaviour to staff, then this will be dealt with under the School's Code of Behaviour and Learning Code

#### **Content Filtering**

St. Paul's Secondary School has chosen to implement the following level on content filtering on the Schools Broadband Network:

Level 5 This level allows access to a wide range (i.e., millions) of educational and other websites but it blocks websites belonging to the 'games' category.

Pupils taking steps to by-pass the content filter by using proxy sites or other means may be subject to disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion.

## **Web Browsing and Downloading**

Pupils may not intentionally visit internet sites that contain obscene, illegal, hateful, or otherwise objectionable materials.

Pupils must report accidental accessing of inappropriate materials in the classroom to their teacher.

Pupils must report accidental accessing of inappropriate materials in school but outside the classroom to their Tutor, Year-Head, Deputy Principal or Principal.

Pupils and staff may not copy information from the internet without acknowledging the creator and referencing the source of the content.

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

Pupils may use the school's internet connection only for educational and career development activities.

Pupils may not engage in online activities such as uploading or downloading large files that result in heavy network traffic which impairs the service for other internet users.

Pupils may not download or view any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

- Use of file sharing and torrent sites is not allowed.
- Downloading by pupils of materials or images not relevant to their studies is not allowed.

## **Email and Messaging**

The use of personal email accounts is not allowed at St. Paul's Secondary School.

Pupils should not use school email accounts to register for online services such as social networking services, apps, and games.

Pupils will not send any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

Pupils should immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature to their Tutor, Year-Head, Deputy Principal or Principal and must not respond to any such communication.

Pupils should avoid opening emails that appear suspicious. If in doubt, pupils should ask their teacher before opening emails from unknown senders

## **Social Media**

The following statements apply to the use of messaging, blogging and video streaming services in St. Paul's Secondary School:

- Use of instant messaging services and apps including Snapchat, Whats Apps, G Chat etc. is not allowed in St. Paul's Secondary School.
- The use of an appropriate blogging platform will be identified by the School where necessary
- Use of video streaming sites such as YouTube and Vimeo etc. is with express permission from teaching staff.

Staff and pupils must not use social media and the internet in any way to harass, insult, abuse or defame pupils, their family members, staff, other members of the St. Paul's Secondary School community

Staff and pupils must not discuss personal information about pupils, staff, and other members of the St. Paul's Secondary School community on social media.

Staff and pupils must not use school email addresses for setting up personal social media accounts or to communicate through such media.

Staff and pupils must not engage in activities involving social media which might bring St. Paul's Secondary School into disrepute.

Staff and pupils must not represent your personal views as those of bring St. Paul's Secondary School on any social medium.

## **Personal Devices**

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

The following statements apply to the use of internet-enabled devices such as tablets, gaming devices, and digital music players in St. Paul's Secondary School:

Pupils are allowed to bring personal internet-enabled devices into St. Paul's Secondary School.

Pupils are only allowed to use personal internet-enabled devices during lessons with expressed permission from teaching staff.

Pupils are only allowed to use personal internet-enabled devices during social time with expressed permission from staff.

## **Images & Video**

Care should be taken when taking photographic or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

At St. Paul's Secondary School pupils 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 not allowed under any circumstances without the permission of the teacher.

Taking photos or videos on school grounds or when participating in school activities is allowed once care is taken that no harm is done to staff or pupils of St. Paul's Secondary School.

Taking photos or videos on school grounds or when participating in school activities is only allowed with expressed permission from staff.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Pupils must not 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 pupils and/or minors is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved. Sharing explicit images of other pupils automatically incurs suspension as a sanction.



## **Cyberbullying**

When using the internet pupils, 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 pupil 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 pupils 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 cyber-bullying even when it happens outside the school or at night.

Measures are taken by St. Paul's Secondary School to ensure that staff and pupils 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 cyber-bullying even when it happens outside the school or at night.

Isolated or once-off incidents of intentional negative behaviour, including a once-off offensive or hurtful text message or other private messaging, do not fall within the definition of bullying and will be dealt with, as appropriate, in accordance with the school's code of behaviour.

The prevention of cyber bullying is an integral part of the anti-bullying policy of our school.

## **School Online Presence**

Webpages 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.

The publication of student work will be coordinated by the school.

St. Paul's Secondary School will use only digital photographs, audio or video clips of 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 not be published on St. Paul's Secondary School web pages or other online platforms.

This policy and its implementation will be reviewed annually by the following stakeholders: Board of Management. This policy is being developed by a working group including Principal, Deputy Principal, teachers, pupils, parents/carers, and representatives of the Board of Management.

The school will monitor the impact of the policy using:

- Logs of reported incidents.

- Surveys and/or questionnaires of pupils.
- Surveys and/or questionnaires of pupils, parents, and teaching staff.

Should serious online safety incidents take place, the Principal will be informed.

The implementation of this Internet Acceptable Use policy will be monitored by the Principal and Board of Management.

This policy and its implementation will be reviewed regularly by the Board of Management.

## **School Strategy for Teaching Staff**

Various technologies are provided and managed by the school and made available to staff to further their professional development and the education of the students in the school. Access to the school's supplied technologies is a privilege and not a right.

Any staff member who abuses this privilege will be immediately excluded from accessing and using the computing facilities. Exclusion from using school technologies 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 in 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.

## **Teacher Use of Networks & the Internet**

- Users must not use the service for the transmission of illegal material. The user agrees to refrain from sending or receiving any materials which may be deemed to be offensive, abusive, indecent, hard-core or pedophile pornography, defamatory, obscene, menacing or otherwise as prohibited by current and future statutes in force.
- The user agrees to refrain from sending or receiving any material, which may be in breach of copyright (including intellectual property rights), confidence, privacy, or other rights.
- If you are in any doubt as the legality of what you are doing, or propose to do, you should either seek independent legal advice or cease that usage.
- Pupils' work should never be shared on social networking sites or websites other than the school website. Sharing or making references to a student's work, especially if it could undermine the student, is not acceptable.
- 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.
- 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 participate in the sending of unsolicited commercial or bulk email, commonly referred to as 'spam'.
- 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.

- Access to the computer network should only be made using the authorised logon name and password.
- The use of USB Sticks / Hard Drives for storage of personal data is prohibited.
- The use of the network to access and/or store inappropriate materials such as pornographic, racist, or offensive material is forbidden.
- In the interest of protecting the network from potential virus activity, the downloading of programs, games, screensavers, and wallpapers from the internet or uploading the same from disc or USB may only be carried out by the ICT Coordinator. This does not prevent users from using images taken and/or saved by them to set their desktop backgrounds.
- Use of the computing facilities for personal financial gain, gambling, political purposes, or advertising is forbidden.
- Copyright of material must be respected, particularly with regard to the download and use of protected images for further use.

### **Use of VS Ware / Office 365**

- In order to protect the information that is accessible on VS Ware / Office 365, users must not divulge their logon details to third parties. Any concerns or queries must be forwarded and dealt by a member of the ICT Team with Administrator rights on the VS Ware / Office 365 system.
- When accessing VS Ware / Office 365 on personal devices, staff should never save /cache usernames or passwords on these devices.
- When accessing VS Ware / Office 365 on personal devices, staff should never download / save documents onto their personal hard drive.

### **Email**

- Teachers will use approved school email accounts for all communications.
- Teacher's use of email is facilitated strictly in an educational context and access to personal email and/or social networking accounts is prohibited.
- Teachers are prohibited from "forwarding" emails from their school account to their personal email address.
- Users must not send any emails that are likely to cause distress or any material which is offensive, indecent, obscene, menacing, or in any way unlawful.
- Users must not use the school network, or Office 365 to send messages or emails to any user who does not wish to receive them.

- The school network must not be used to send or distribute unsolicited commercial mail, commonly known as 'spam', in bulk or individually.
- Users, as senders of emails, must not use false mail headers or alter the headers of mail messages in such a way as to conceal the identity of the sender.
- Where emails and attachments contain sensitive personal information, staff are required to encrypt these emails. Attachments including sensitive personal information should be password protected i.e., ensuring only the recipient(s) with a password can open and access the contents of the email.
- Staff will not save copies of personal data to their own personal computers, phones, tablets, USB sticks, Hard Drives.

Signed: \_\_\_\_\_  
(Chairperson Board of Management)

Signed: \_\_\_\_\_  
(Principal)

Date: \_\_\_\_\_

Date: \_\_\_\_\_

This policy was adopted by the Board of Management on **14<sup>th</sup> October 2021**

### Permission Form

I agree to follow the school's Acceptable Use Policy on the use of the Internet. I will use the Internet in a

responsible way and obey all the rules explained to me by the school.

Student Signature: \_\_\_\_\_ Parent/Guardian: \_\_\_\_\_

Date: \_\_\_\_\_

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access the Internet. 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: \_\_\_\_\_

Please review the attached school Internet Acceptable Use Policy, and sign and return this permission form to the Principal.

School Name: St. Paul's Secondary School

Name of Student: \_\_\_\_\_ Class/Year: \_\_\_\_\_

Student: \_\_\_\_\_