STP WIRELESS LEARNING ENVIRONMENT

The OCSB offers a secure wireless environment for all students and staff at St. Paul High School that allows for improved student access to educational resources over the Internet. Students may be permitted to use personally owned devices (PODs) to connect to the World Wide Web for educational purposes, through the board's wireless network.

PODs include but are not limited to the following devices: portable computers, smart phones, and music player devices. Prior to students accessing the school wireless network, whether from our school devices or from the students PODs, students and parents must sign the Acceptable Use of Technology Agreement and Student Declaration for the Use of PODs. While accessing the network, students are required to follow the OCSB Computer and Internet Use Policy and the St. Paul Acceptable Use of the Wired and Wireless Network (Network) Guidelines

e-Learning

E-Learning options are available to some students who for various reasons require courses beyond what is available through the school. Students must meet with a guidance counselor to determine whether and e-Learning course is the appropriate delivery method for their timetable.

Computer and Internet Use Policy

To gain access to the OCSB's network and the Internet, all students must agree to the following terms and conditions:

a) Network users are responsible for appropriate behaviour on the Board data networks, as outlined in the school code of conduct.

b) Access to network services is a privilege given to users who agree to act in a considerate and responsible manner. That access entails responsibility. Inappropriate use may result in a suspension or cancellation of access privileges. School administrators and staff supervisors will deem what is inappropriate use.

c) Network users are expected to abide by the generally accepted rules of network etiquette and conduct themselves in a responsible, ethical, and polite manner while online.

d) Users are only permitted to use network resources for school purposes.

e) Network users are not permitted to transmit, request, submit, or publish any defamatory, inaccurate, abusive, obscene, profane, pornographic, threatening, offensive, racist, illegal material.

f) Network users may not willfully access any files or content that may damage, compromise, violate, infiltrate or in any way negatively affect the Board computers, electronic devices or network or those of other users.

g) Students, upon accidentally arriving at an inappropriate site, must follow the procedure ("Stop, Back, Tell" – Click the stop button, click the back button, tell the teacher).

h) Physical or electronic tampering with computer resources is not permitted. Damaging computers, or compromising security on computer systems, or computer networks may result in cancellation of the user's privileges.

i) Network users must respect all copyright laws that protect software owners, artists and writers. Plagiarism in any form is not permitted.

j) Security on any computer system is essential. Students aware of any problem in the school's computers, network, or Internet connection, should notify the system administrator and/or teacher. Students must not demonstrate any potential security problem or risk to others. Using someone else's password or accessing anyone else's electronic or online content without their permission is prohibited.

k) Network users should be aware that their use of Board resources is monitored and recorded. Information Technology staff employs the use of Internet tracking and filtering software to control and monitor Internet access.

l) The Ottawa Catholic School Board makes no warranties of any kind, whether expressed or implied, for the service it is providing. The Board assumes no responsibility or liability for any phone charges, line costs or usage fees, nor for any damages that a user may suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions. Use of any information obtained via the Internet is at the user's own risk. The Board specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Acceptable Use of the Wired and Wireless Network (Network) Guidelines

In addition to the Computer and Internet Use Policy, each time students access the network either from our school devices or from the students PODs, students agree to the following:

1. Students are expected to follow the guidelines for Social Media Sites and On-line Conduct.

Social Media Sites and On-line Conduct

The use of social media can be effective communication tools. Where appropriate, school staff may choose to participate in school sanctioned online activities (example – A school site to promote a social justice activity or a school team). School sanctioned online sites will have a minimum of two school staff members with administrative privileges, where available.
Students are reminded that their online conduct should be similar to their face to face conduct and at all times should respect the school code of conduct.

Students may be disciplined, including suspension or expulsion, if their online behaviour results in a

disruption to the school environment or negatively impacts our Catholic school climate. Online threats may be determined to be a criminal offence and as such, they may be reported to the school resource officer.

Students are not permitted to digitally photograph or record audio or video of school activity without first obtaining permission from those involved. A teacher or administrator may give permission for the digital recording of school activities and events (ie. sports game, spirit assembly, special presentation) where the participants are aware that they may be recorded. The online digital posting of classroom activity violates the privacy of others who have not granted permission to be recorded. The online digital posting of inappropriate student interactions (ie. student fight) is likely to have a negative impact on the school climate. As such, in both instances, the online digital posting requires teacher or administrative approval prior to being posted. Users shall remain anonymous (i.e. true identity not revealed) when publishing content on the Internet. Students will not use their full name (first name only), phone number, home address, other users' full names, or any other information that can lead to the real identity of the user.

2. Users shall bring known or suspected abuses to the attention of any staff member.

3. St. Paul H.S. will not be held liable for any damage that may occur to the PODs as a result of accessing the network nor will it be held responsible for any physical damage, loss, or theft of the PODs.

4. St. Paul H.S. reserves the right to inspect running programs or suspicious behaviour on a POD, at any time, while connected to any network.

5. St. Paul H.S. makes a distinction between the use of the network in the direct teacher supervision areas (classrooms, gyms, library) and the school common areas (cafeteria, hallways, other). In the classroom setting, the use of PODs for educational purposes will be

at the discretion of the classroom teachers. In the school common areas, students are allowed to use the PODs primarily for educational purpose. Students may use PODs during their leisure time but must be mindful of the network etiquette and our Catholic Graduate Expectations. In addition, they are expected to refrain from using games of inappropriate or violent nature.

6. At the 7 & 8 levels, students will not be permitted to use PODs during the school day. Teachers are being encouraged to explore ways of integrating technologies into their teaching.

Any violation of these guidelines constitutes grounds for immediate removal or restriction of network access and may result in further disciplinary action. Evidence or strong suspicion of a violation may result in the suspension of a user's right to network access, pending further clarification or investigation, and in the confiscation of the students PODs.

Cyber-bullying

Neither the school's network nor the broader Internet (whether accessed on campus or off campus, either during or after school hours) may be used for the purpose of harassment. All forms of harassment in cyber-space, often called cyber-bullying, are unacceptable.

Cyber-bullying includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another person by sending or posting inappropriate and hurtful e-mail, instant or text messages, digital pictures or images, or website postings (including blogs).

All reports of harassment in cyber-space will be investigated. Sanctions may include, but are not limited to, the loss of computer privileges, detention, and suspension from school. Safe schools legislation mandate that schools deal with any action that has a negative impact on the school climate or an individual at the school. Cyber-bullying will not be tolerated even if it is done away from the school.