ORANGEVILLE CHRISTIAN SCHOOL

Policy: Acceptable Use of Technology

Policy Approved: 2009, Revised September 2025

PREAMBLE

With information technology and all related technology expanding and advancing rapidly, it is becoming increasingly important to bear in mind that our created ability to develop and use tools and information must be managed responsibility and with God-honouring intentions. Christians have a duty to not only discern tensions that may exist when using technology, but to establish boundaries or limits.

The purpose of this policy, which applies to all students of the school, is to set out conditions and guidelines for the use of technology in Orangeville Christian School (the "School") including:

(a) all School-owned or controlled (or used by the School under license for the School's purpose and activities) database/records systems, networks, cabling, School-associated cloud services, School email, voicemail, fax transmissions, and the use of and access to the School intranet and internet (collectively called the "School Network") and

(b) all computers and mobile or portable devices, hardware, software using School technology or on School premises.

"School Technology" is any of the above which is owned or controlled by the School, or used by the School under licence, for the School's purpose and activities. Together, the School Technology and School Network are referred to as the "School Network and Technology"

This policy has also been established to create responsible and productive boundaries with social media when representing or referring to the school. It sets out conditions for blogging and posting online content with respect to students of the School.

This policy may change from time to time, and the School will inform students of updates to the policy. Each student shall abide by the most-current version of the policy and is expected to become familiar with the policy and to adhere to it at all times.

POLICY

All School Network and Technology belongs to the School and is owned by the School.

The School Network and Technology is available for instruction and research by students, teachers, and administrators. The use of these facilities is a privilege and must be in support of the educational objectives of the School.

The use of hardware, software and technology, such as workstations, peripherals, wireless networks, and web sites may be monitored and logged. This includes any data transmitted on the School Network,

including hardware identification information, or data transmitted on personal devices owned by students using the School Network, or on School premises.

While the School endeavours to respect privacy, the School monitors access on a day-to-day basis and may review any data as needed for security, maintenance, or legal investigative purposes.

All students must respect and comply with all federal, provincial, and municipal laws, including the Criminal Code and Copyright Act, which includes respecting the rights of copyright owners, software manufacturers, and abiding by the terms of all licence agreements relating to the School Network and Technology. Failure to comply with the terms of licence agreements or engaging in other conduct that violates this policy may be subject to disciplinary action, up to and including expulsion from the School.

CODE OF CONDUCT

Each student has a responsibility to uphold the School's Code of Conduct and to use all technology, including the internet, in a responsible and productive manner. Students must use the School Network and Technology, even when using personal electronic devices, in a responsible manner consistent with the goals of the School. The School Code of Conduct applies to online behaviour just as much as it does to personal interactions. Unauthorized or irresponsible behaviour will result in the loss of School Network and Technology privileges and may include other sanctions, up to and including expulsion from the School.

All students must refrain from using profane, abusive or impolite language to communicate when accessing and using the School Network and Technology, or when using personal devices on School premises. As well, no materials should be accessed or distributed which are not in line with the rules of school behaviour and set out in the Code of Conduct.

Cyber-bullying violates the basic tenet that all students are entitled to feel comfortable and safe. Cyber-bullying is a criminal offence and will not be tolerated. This includes the use of email, text messages, instant messaging, social media posts, and/or defamatory content on websites to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others, or that has the reasonably foreseeable result of harming others.

In addition, students must not use either the School Network and Technology or their own personal electronic devices for:

- creating, processing, downloading, distributing, accessing or sharing illegal, offensive, pornographic and/or inappropriate materials;
- knowingly accessing sites containing material that is discriminatory or inappropriate to a school environment;
- accessing, downloading, storing, or sharing media files, including music and video files or any other materials that are illegal, offensive, obscene, inappropriate or that are not intended for School purposes;
- sending or receiving defamatory, abusive, obscene, profane, sexually oriented, threatening, or racially offensive messages;
- knowingly creating, exchanging, transmitting and/or downloading of messages, content, or data that are offensive, harassing, obscene, libelous, abusive, discriminatory, threatening, or encourage violence;

- accessing any other person's social media accounts, email, data, or personal information without express prior written permission from that person;
- impersonating any other person's online profile or presence or misrepresenting themselves online;
- recording anyone else without their express prior permission, and/or sharing recordings through any means (social media applications, websites, etc.), including temporary recordings made and shared on mobile applications such as Snapchat;
- attempting to or actually violating or infringing any other person's intellectual property and related rights (including copyright);
- uses that violate any federal or provincial laws, copyright, intellectual property or other laws, guidelines or agreements;
- conducting, advertising or soliciting business or commercial activities which are unrelated to School activities, including personal services or alcohol or drug (including cannabis) related products or services, unless prior written permission has been obtained from the applicable School authorities;
- computer-hacking and related activities, including installing or downloading software on the School Network and Technology without prior written permission from the applicable School authorities.
- intentionally installing or transmitting any kind of malicious software, which is a serious offense, both within the school and under Canadian law;
- creating, accessing or using malicious websites, chat rooms, "spam", malicious messages to send to others;
- engaging in other wasteful or forbidden use of the School's electronic resources;
- attempting to circumvent any form of security, be it to log into a wireless network, access a blocked web site, or access any computer resources they are not permitted to use as well as attempting to disable or compromise the security of information contained on the School Network and Technology, and applicable external networks;
- uses that are malicious, unethical, or in violation of accepted community standards or School guidelines and policies, such as cheating or "leaking" School test materials or confidential information;
- attempting to interfere with or delete data or applications, unplug cables, or install any new software on School equipment;
- mistreating, abusing, vandalising or destroying School equipment, including hardware or software to which they are granted access.

PASSWORDS

Students shall access the School technology, network and IT facilities only with an authorized username and password as provided by the School. The use of passwords is intended to ensure that only authorized individuals have access to School Network and Technology, and the private and confidential information they contain or provide access to.

Students who are granted access to electronic accounts, usernames and passwords by the School are held responsible for all activity that takes place within their account, unless it can be otherwise proven in exceptional circumstances.

Each student must keep their School-related account passwords and access codes secret. Under no circumstances should students share their passwords for the School Network and Technology or for any School resource with anyone other than authorized school IT support staff or authorized School officials. This includes, but is not limited to, computer login information, email account passwords and login information, wireless access passwords, or login and access information to any websites, platforms, forums, networks, or database students sign up for as part of a School-related class, activity or purpose.

Passwords should not be posted where other people might see them. Every student must take reasonable precautions to protect the integrity of the School Network and Technology to prevent unauthorized access by others. For example, before leaving computers or mobile devices unattended, students must:

(a) not leave School Technology unsecured or unattended unless necessary; and

(b) log out of their workstations and devices when finished with them.

PRIVACY

Each student must recognize that they have a limited expectation of privacy regarding access or use of the School Network and Technology, even when this access or use is restricted to School activities and the information is stored on School computers or devices.

The School has the right, but not the obligation, to inspect any computer or computer systems, and to monitor the use of any of the School Technology, including, without limitation, inspecting the contents of voicemail, social media, and email communications. Students will not necessarily be notified when such monitoring is to take place, or whether monitoring has occurred. In certain situations, the School may be compelled to access, read, copy, reproduce, print, retain, move, store, destroy and/or disclose messages, files or documents stored on or sent over the School Network or using School Technology. These situations may include, but are not limited to the following:

(a) in the course of regular maintenance of School Network and Technology;

(b) in the event of a request for documents as part of litigation or similar proceedings; or

(c) where the School has reason to believe that the School Network and Technology are being used in violation of this Policy.

Students should not intentionally view another user's documents, email, or other private materials without their consent. If another user fails to log off a public computer, the discoverer should immediately log out of the account if no documents are open. If there appear to be work that needs to be saved, ask the staff member responsible for that computer to take care of it.

Unauthorized access by any student of another individual’s electronic information is a violation of the School policy. Access by a student of another individual’s electronic information will only be permitted with written approval from the Principal.

Students must not disclose personal contact information about other students, staff members or members of the School community. Personal contact information includes physical or electronic addresses, social media account information, identities, links or “handles”, pseudonyms, telephone numbers and other such personal information. Publication of pictures of individuals or a group requires the informed permission of all the individuals involved and, in the case of minors, of their parents or guardians.

Students must not publish photographs of students other than on the School websites, on School social media websites, pages or accounts, or in School publications even with express informed consent of all

those involved, unless prior written consent and approval has been obtained from the relevant School authorities.

COPYRIGHT

Students are not permitted to illegally access, download, store, or share software, media, books or any other materials or copy, transfer, rename, add or to delete information or programs belonging to others, unless given the express written permission to do so by the owner.

Examples of copyright violations may include, but are not limited to, copying a picture, making illegal copies of software or music and/or reproducing part of a third-party text and claiming credit for authoring that work.

Certain underlying resources which are used with the School Network and Technology and equipment may be subject to copyright, intellectual property laws and other laws—these may not be in the public domain or free for use. For instance, 3D printing files (in .STL or other formats) and other file formats (e.g., graphics, vectors, images, sound and video clips, including materials found on social media platforms such as YouTube, Snapchat, Reddit, etc.) created by others may be copyrighted and owned by someone else. Students may need to seek permission to use such files, even if they are using only a part of such files. Software and resources downloaded must only be used under the terms and conditions specified by the creator or owner of the resource. If students intend to use materials created by someone else in their own work, they must ensure to cite appropriately.

SCHOOL TECHNOLOGY RULES AND PROCEDURES

Students must treat all School equipment with care and make all reasonable efforts to keep equipment in good condition. This means knowing and following computer and IT lab rules and procedures. Prior to having any media, including open source software, placed on the School Network, students shall obtain the prior approval of the Principal or designate and provide evidence of purchase of the software or evidence that the software is available legally and for free, a copy of the license terms, and a description of the School purposes for which the media or software will be used.

In exchange for being permitted to use and access the School's computer facilities and spaces, the following guidelines apply to students:

- Treat all School-owned property with care and respect. Do not deface, vandalise or destroy the School's equipment and resources.
- Students must read all safety guidelines and instructions when using School technology and equipment (e.g. 3D printers, virtual or augmented reality equipment) and wear appropriate safety gear and clothing (where required). The School shall not be responsible for injuries caused due to misuse or improper use of such equipment.

USE OF PERSONAL ELECTRONIC DEVICES

Teachers have sole discretion to allow or disallow classes or individual students to use laptop computers, mobile devices, or internet access at any given time during a class. Failing to comply with a teacher's decision may lead to the student's equipment being temporarily confiscated and/or having their wireless account and access to the School Network suspended.

Cameras and personal devices present a personal privacy issue for the School community. It is recognized that most personal devices include camera capabilities, and that cameras may be used for legitimate classroom purposes. Students who are using a camera in violation of applicable School rules will have their camera/device confiscated by school administration and/or be subject to appropriate disciplinary action. This includes all cameras which can be attached to clothes or accessories (such as GoPros), unmanned remote operated devices (including drones) and any wearable technology (including all attachable devices that can monitor, track or record).

The School shall not be responsible for the theft, loss or damage to any personal electronic devices brought to school by a student.

EMAIL AND SOCIAL MEDIA

Email is often used as a resource for both class and student activities and students are responsible for checking their email in a timely fashion when directed to do so by a teacher or other school staff.

Students may forward their school email to another account address but must take care to make sure any sent email includes their name if their email address doesn't clearly identify them. All students are responsible for personal equipment connected to the School Network, including if such equipment is connected off School premises (e.g., connecting to cloud-based servers).

Use of the School Network requires the acceptance of terms and conditions on the Network sign-in page. Students are expected to review the terms whenever updates or revisions to the terms are communicated by the School.

In addition to the above requirements, students should adhere to the following general guidelines for appropriate and safe online conduct:

(a) Be aware of what is posted online. Social media venues are very public and what is posted leaves a digital footprint. Students should not post or repost anything that they would not want friends, parents, teachers or a future employer to see or that may reflect poorly on them, their friends, or the School.

(b) Follow the School Code of Conduct when writing online. It is acceptable to disagree with someone else's opinion; however, it must be done in a respectful way. Make sure that criticism is constructive and not hurtful—what is inappropriate in the classroom is inappropriate online. Avoid impulsive, inappropriate or heated comments.

(c) Be safe online. Never give out anyone's personal information, including but not limited to last names, telephone numbers, addresses, exact birthdates, credit card numbers, pictures, etc. Do not share passwords with anyone besides teachers and parents.

(d) Do not post, publish or display any defamatory, abusive, obscene, threatening, intimidating, or racially offensive material.

(e) Alert school staff if students are being threatened, intimidated or bullied online.

(f) Be transparent and authentic.

(g) Be cautious when interacting with others online. Students should not respond to any messages that make them feel uncomfortable, threatened, or intimidated. If an online interaction makes a student uncomfortable or is inappropriate, they should not hesitate to tell their teachers and parents/guardians immediately.

(h) Set and maintain appropriate privacy settings by choosing settings that limit what others can do.

(i) Monitor regularly all content posted on social media accounts and remove anything that is inappropriate.

This Acceptable Use of Technology Policy approved by the Board of Orangeville Christian School, September 2025.