



STUDENT USE OF DIGITAL DEVICES

Updated: 7 April 2025

Pompallier Catholic College can provide students access to a wired or wireless network, and the option of bringing in a personal electronic device as a means to enhance learning and teaching. The purpose of these guidelines is to ensure that students recognise the expectations that the school imposes on their use of digital devices in the school context.

GUIDELINES

The use of digital devices in the school environment is at the discretion of the school.

1. That connection of a device to the school network can be revoked at any time.
2. Students must obtain teacher permission before using a digital device during classroom instruction.
3. Student use of a device must support the instructional activities currently occurring.
4. Students must turn off and put away a device when requested by a teacher.
5. When a teacher believes that the possession of a device endangers the safety of any person or detrimentally affects the learning environment; students shall surrender the computer or electronic device for inspection and/or retention. The device may be retained in accordance with the Surrender and Retention Policy 2024.

Responsibility

1. Pompallier Catholic College accepts no responsibility for personal property brought to the school by students.
2. Students who choose to bring their personal devices to school assume total responsibility for them.
3. Students should take all reasonable measures to protect against the theft or damage of their personal equipment. The school shall not be responsible for devices that are stolen or damaged.
4. The school recommends that owners of devices seek appropriate insurance cover.

Internet / Network Access for students

1. Students will be assigned a school email account, in order to access educational electronic resources.
2. Students shall use only the assigned username and password to access the Internet.
3. Internet access is monitored. Students will be held responsible for their use of the Internet.
4. All network activity must be legal.
5. The Internet is to be used for scholarly research and as a means of obtaining needed information.
6. Sites that are not aligned with our Special Character are inappropriate to view and may result in the loss of access and/or other action.
7. No computer programmes (executables), pornography, or copyrighted material, may be accessed or distributed over the network.

8. Students shall access only appropriate information, images and data, and use appropriate language, images and information.
9. For security and network integrity, VPNs should not be used at school.
10. Never view, use, or copy passwords of another user.
11. Never distribute personal information regarding yourself or anyone else, to anyone online - such as, but not limited to: phone numbers, addresses, last name, photos or videos of anyone.
12. Immediately report threatening, discomforting, indecent or inappropriate materials, found on the internet or in a file, to a teacher or someone in authority.

Recommendations

Users should take the following physical security preventative measures:

- Your digital devices should **never** be left unattended for **any** period of time.
- Digital devices must not be left in view outside of instructional usage.
- Unattended devices shall be deposited at the Student Centre.

Access Control and Authentication

To use a device within the school's digital environment, students must use their assigned logon.

No student shall knowingly gain access to, or attempt to gain access to, any computer, computer system, computer network, information storage media, or peripheral equipment, without the consent of authorised school personnel.

Consequences for Inappropriate Device Use

Failure to adhere to the technology conditions and rules as outlined above will result in disciplinary action.

Violations of any of these Guidelines can result in retention of devices in compliance with the school policy and the Education and Training Act 2020.