Pompallier Catholic School
General Cybersafety Rules

These general rules have been developed to support the important school cybersafety initiatives outlined in Section A: Important Pompallier Catholic School Cybersafety initiatives.

1. Staff and students are required to sign use agreements with the school.
1.1 Please sign the last page of this use agreement and return it to the school office.
NB The entire document should be kept to refer to later, including a copy of the signed form.

2. Use of any ICT must be appropriate to the school environment
2.1 **For educational purposes only**. The school's computer network, Internet access facilities, computers and other school ICT equipment / devices can be used only for educational purposes appropriate to the school environment. This rule applies to use on or off the school site. If any other use is permitted, the school will inform the user/s concerned.

2.2 **Permitting someone else to use school ICT.** Any staff member or student who has a signed use agreement with the school allows another person who does not have a signed use agreement as per point 1 (above) to use the school ICT, is responsible for that use.

2.3 Privately-owned ICT. Use of privately-owned/leased ICT equipment / devices on the school site, or at any school-related activity must be appropriate to the school environment. This includes any images or material present/stored on privately – owned/leased ICT equipment / devices brought onto the school site or to any school-related activity. It also includes the use of mobile phones. Any queries should be discussed with the Principal.

2.4 **Responsibilities regarding access of inappropriate or illegal material.**
When using school ICT, or privately-owned ICT on the school site or at any school-related activity, users must not:

- Initiate access to inappropriate or illegal material
- Save or distribute such material by copying, storing or printing.

In the event of accidental access of such material, users should:

1. not show others
2. close or minimize the window
3. report the incident
   - Students should report to a teacher immediately
   - Staff should report such access as soon as practicable to the Principal

2.5 **Misuse of ICT.** Under no circumstances should ICT be used to **facilitate** behaviour which is either inappropriate in the school environment or illegal.

3. Individual password logons (user accounts)

3.1 Individual user name and password. If access is required to the school computer network, computers and Internet access using school facilities, it is necessary to obtain a personal user account from the school.

3.2 Confidentiality of passwords. It is important to keep passwords confidential and not shared with anyone else.

3.3 Access by another person. Users should not allow another person access to any equipment / device logged in under their own user account, unless with special permission from senior management. (Any inappropriate or illegal use of the Pompallier Catholic School's computer facilities and other school ICT equipment / devices may be traced by means of this login information.)

3.4 Appropriate use of email. Those provided with individual, class or group e-mail accounts are expected to use them in a responsible manner and in accordance with this use agreement. This includes ensuring that no electronic communication could cause offence to others or harass or harm them, put the owner of the user account at potential risk, or in any other way be inappropriate in the school environment.

4. Disclosure of personal details

4.1 For personal safety, users should be very careful about revealing personal information about themselves, such as home or email addresses, or any phone numbers including mobile numbers. Nor should such information be passed on about others.

5. Care of ICT equipment / devices

5.1 All school ICT equipment / devices should be cared for in a responsible manner.

5.2 Any damage, loss or theft must be reported immediately to the ICT Manager.

6. Wastage

6.1 All users are expected to practise sensible use to limit wastage of computer resources or bandwidth. This includes avoiding unnecessary internet access, uploads or down loads.

7. Connecting software / hardware

7.1 Users must not attempt to download, install or connect any unauthorized software or hardware onto school ICT equipment, or utilise such software/hardware. This included use of such technologies as Bluetooth, infrared, and wireless, and any other similar technologies which may be developed. Any user with a query or a concern about this issue should speak with the Principal.

7.2 In a special case where permission has been given by the ICT Manager to connect or install privately-owned equipment/devices or software, it is with the understanding that the school may scan this equipment/device/software, it is with the understanding that the school may scan this equipment/device/software at any time thereafter as part of a regular or targeted security check, such as for viruses.

8. Copyright and Licensing

8.1 Copyright laws and Licensing agreements must be respected. This means no involvement in activities such as illegally copying material in any format, copying software, downloading copyrighted video or audio files, using material accessed on the internet in order to plagiarise, or illegally using unlicensed products.

9. Posting material

9.1 All materials submitted for publication on the Internet/Intranet should be appropriate to the school environment.

9.2 Such material can be posted only by those given the authority to do so by senior management.

9.3 The Principal should be consulted regarding links to appropriate websites being placed on the school Internet/Intranet (or browser homepages) to provide quick access to particular sites.

9.4 There is only one official website relating to the school with which there should be involvement unless approval has been given by senior management.

10. Queries of concerns

10.1 Staff and students should take any queries or concerns regarding technical matters to the Principal.

10.2 Queries or concerns regarding other cybersafety issues should be taken to the Principal.

10.3 In the event of a serious incident which occurs when the Principal are not available, another member of senior management should be notified immediately.