STUDENT ICT ACCEPTABLE USE POLICY

CATEGORY

Operational

BACKGROUND

The Penrhos College network, internet electronic communication facilities are maintained by the College to assist in the teaching/learning and administrative functions of the school.

All students (Years 5-12) are provided with monitored access to these facilities.

Access to the facilities is provided by the Technical Support Department of the College, where user accounts and passwords are issued. Ongoing access to these facilities is dependent on signed agreement to this Policy.

The integrity of the system relies upon the security of passwords and responsible behaviour by users. Responsible behaviour is outlined in the Policy Statement.

POLICY STATEMENT

1. Network, internet and electronic communication using College resources will be used for educational purposes.
2. The College Internet is a filtered and monitored system. Bypassing the College's filtering systems whilst on campus using the College provided notebook (e.g., via wireless internet cards or dongles) is not permitted. The use of the internet via personal mobile phones is permitted before and after school hours only. Students accessing the internet on mobile phones through personal data plans must show responsible behaviour in line with the College values and abide by the College Mobile Phone policy. No other personal devices including smart watches are permitted on campus.
3. Students are expected to show responsible behaviour when using network, internet, and electronic communication on any device, in accordance with the accepted standards of behaviour within the College. Users are held responsible for their own actions when using network, internet and electronic communication.
4. Any communication among members of the College community must be in accordance with College policies.
5. Parents will be notified of any unacceptable use of network, internet, and electronic communication. This will also result in consequences, according to the appropriate behaviour management policy.
6. Students are expected to refer any cyber safety related issues to a parent, member of the Pastoral Care team, staff member, or the College online reporting system on the Pastoral Page of the portal.

Some examples of such unacceptable use are listed below:

- Bringing into the College any material gained from the **internet or elsewhere** which **is likely to be considered inappropriate to the College Values. This includes illegally obtaining images, video, audio files as well as applications.** Any such materials detected on the College notebook will be removed.
- Deliberately accessing sites **which are likely to be considered inappropriate to the College Values**
- Posting personal information about yourself, another student or member of the College Community on the internet such as your name, birth date, address, telephone number, current location and/or school
- Posting text, audio, photographs or video on the internet which brings the College or community members into disrepute (e.g., using inappropriate language in email communication or on Instagram, Snapchat, Facebook and other social networking sites)
- Posting inappropriate or unauthorised material of yourself or a member of the College community on the Internet (e.g., Facebook, You Tube, Instagram, Snapchat, Music.ly)
- Using proxy sites to bypass College filtering and monitoring systems
- Using College resources to harass or bully others
- Revealing your account details (username & password) to others. Using any other staff or student account details (username & password) to gain unauthorised access to network or internet sites
- Invading the privacy of individuals (e.g., using another person's notebook without their consent)
- Posting personal communications in someone else's name (e.g., setting up an online profile in the name of a staff member or another student)
- Posting anonymous messages and spreading rumours
- Destroying the data of another user
- Accessing the network on behalf of family members or friends
- Using unauthorised copies of commercial software
- Using the network for any illegal activity, including violation of copyright or other contracts (e.g., peer to peer file sharing software)
- Corrupting or disrupting equipment or system performance
- Using the network for financial or commercial gain
- The creation or forwarding of scams, spam, junk mail, chain mail or any other unsolicited electronic communication

7. Users are not permitted to download any software from the College Network or internet other than copyright-free audio, fonts, graphics, video, sound or text material required for educational use. Public domain and shareware software should not be downloaded due to the danger of malware and possible copyright infringements. Students should see the Technical Services Staff (M8) if there is software that they would like to install on their notebook.

8. The College acknowledges the age guidelines of social networking sites such as Instagram, Facebook, Snapchat, etc. Therefore, the College **does not condone** the use of Instagram and similar sites by **students who do not meet the age requirements set by that site, app or software**. Secondary students who are of age and choose to have social media accounts should set their account to private and turn off GPS location settings, for their safety.

9. All data coming from or being received through the College internet account or being stored on the College network should be considered non-private. Please note that this includes all electronic communications.

10. Students must respect the privacy of College employees. For example:
    a. Students must not add College staff as friends or contacts on any social networking site, other than those designated by the College. These will be for educational purposes only.
    b. Students must not contact College staff at their private residence; instead use the College provided email system.

11. As per their Conditions of Use, some websites, software and applications require parental permission. Where the usage of websites, software and applications meets their Conditions of Use, Australian Privacy Laws and the College's policies, the parental signature below indicates agreement to their daughter's use of those sites, software and applications.

12. Students are responsible for managing and storing their own data correctly. All classwork must be stored in the Documents folder where it is automatically synchronized to College servers. Students are responsible for backing up all data stored in other locations; such as the Pictures, Video and Music folders, the desktop, the local C drive or OneDrive.