Peregian Beach College Acceptable Use of ICT Policy

Purpose:	The purpose of this policy is to establish clear expectations and guidelines for the responsible, ethical, and secure use of all ICT resources within Peregian Beach College, including College-owed ICT resources as well as personal ICT devices when they are used for College-related activities.	
Scope:	This policy applies to all users of ICT at Peregian Beach College, including staff, students, volunteers, authorised guests, and contractors.	
Status:	Approved	**Supersedes:** 2024
Authorised by:	Board Chair	**Date of Authorisation:** January 2025
References:	• Privacy Act 1988 (Cth) • Copyright Act 1968 (Cth) • Australian Privacy Principles • The Australian Student Wellbeing Framework • National Principles for Child Safe Organisations • eSafety Toolkit for Schools • Queensland Government Department of Education Use of ICT systems procedure • Staff Code of Conduct • Privacy Policy • Complaints Handling Policy	
Review Date:	Every 2 Years	**Next Review Date:** January 2027
Policy Owner:	College Board	

DEFINITIONS

- **Acceptable use**: Use of technology that aligns with the values and purposes of the College and the intent of this policy, complies with relevant laws and regulations, and respects the rights of others.
- **AI tools**: Computer programs that utilise machine learning algorithms and other advanced techniques to mimic human cognitive abilities like reasoning, pattern recognition, and

learning from data. These tools can generate creative content, assist with problem-solving, and automate certain tasks.

- **Copyright**: Legal protection granted to original creative works.
- **Cyberbullying**: Repeated online harassment or intimidation targeting an individual.
- **Data**: Any information stored or transmitted electronically, including personal or sensitive information of students and staff.
- **ICT:** Information and Communication Technology. Refers to all technology provided by the College used for collecting, storing, processing, transmitting, and communicating information, including computers, networks, software, applications, and internet access, and personal devices used for College-related activities.
- **Network resources**: Hardware and software infrastructure supporting the College's technology network.
- **Personal device**: Any electronic device owned by a user that is brought to school or used for College-related activities, such as laptops, phones, tablets, smart watches, etc.
- **Plagiarism**: Using someone else's work or ideas without conferring appropriate credit.
- **College-related activities**: Any activity connected to the College, including classes, breaks, assignments, clubs, extracurricular activities, incursions, excursions, and online communication of teachers and students.
- **User**: Any individual authorised to use College ICT, including staff, students, volunteers, authorised guests, and contractors.

ACCEPTABLE USE OF ICT

General Principles

- All ICT use must be responsible, ethical, and legal, respecting the rights and dignity of others.
- ICT should be used to support learning, communication, and collaboration within the school community.
- ICT should be used in a way that maintains a safe and productive learning environment for all.
- To ensure the responsible and safe use of the College's network, Peregian Beach College reserves the right to monitor and maintain appropriate records of network activity (e.g. email, web browsing, file sharing). This monitoring is conducted in alignment with applicable laws to protect the College community and maintain a secure learning environment.

Online Conduct

- Using ICT to engage in any illegal activity, such as hacking, accessing or distributing illegal content, or participating in online scams is strictly prohibited.
- Users must not engage in any online behaviour that is intended to intimidate, humiliate, threaten or harass another person, including sending offensive messages, excluding others from online groups with the intent to ostracise, spreading false or harmful information, or impersonating others.

- Sharing content online that is hateful, discriminatory, promotes violence or illegal activities, or expresses discriminatory views based on protected characteristics such as race, religion, gender, sexual orientation, disability, or any other personal attribute is strictly prohibited.
- Users must not engage in activities that violate community standards of decency and professionalism regarding online content. This includes accessing, viewing, or distributing materials of a sexually suggestive or exploitative nature.

Access and Authorisation

- Access to College technology is granted on a privilege basis and for approved College-related purposes only.
- Limited personal use of College technology may be permitted for staff members during off-duty hours and within the acceptable use parameters outlined in this policy, as long as it doesn't interfere with official duties and incur more than negligible costs.
- Downloading and installing unauthorised software using College technology, including games, gambling software, pirated software, or applications that bypass school security measures or disrupt network performance, is strictly prohibited.
- Users must only access College technology using their own authorised accounts. Sharing of authorised accounts or passwords is strictly prohibited.
- Accessing data or systems that users are not authorised to access, or attempting to bypass security measures to gain unauthorised access is strictly prohibited.
- Users must not share confidential information with unauthorised individuals or organisations.

Data Security and Privacy

- Users should be aware of the risks of online activity and take steps to protect their own data and privacy.
- Users must not collect, store, or share personal information about others without their consent.
- All personal information, including sensitive information, must be handled confidentially and with appropriate security measures to protect against unauthorised access, misuse, or disclosure.
- Users must report potential data breaches or security vulnerabilities in alignment with the PBC Privacy Policy and Data Breach Response Plan.

Online Communication and Behaviour

- All online communication must be respectful, courteous, and professional.
- Cyberbullying, harassment, and discrimination are strictly prohibited.
- Users must not engage in offensive or illegal online activities.

Content Creation

- Users must respect copyright laws, avoid plagiarism, and not use ICT in any way that impacts on the academic integrity of work produced.
- Using copyrighted materials without permission, such as downloading or sharing music, movies, software, or other copyrighted works without the owner's consent is strictly prohibited.
- Submitting work that is plagiarised is strictly prohibited.
- Users should be mindful of the potential impact of their digital content on others.

Network and Internet Use

- The College network and internet resources are valuable tools for learning and communication. All users are responsible for using these resources efficiently and prioritising activities that support educational goals.
- Users must be mindful of data download and upload limitations when accessing online content or engaging in network activity, and consider the impact their usage might have on others' access and the overall network performance.
- If users' activities require significant data usage, they should consult with relevant staff to explore options and ensure responsible resource allocation.
- Overloading the network with excessive bandwidth usage, downloading large files for personal use during peak hours, or engaging in activities that disrupt others' access to network resources must be avoided.
- Accessing websites or online services that contain harmful content or present security and privacy concerns is strictly prohibited.
- Using College network resources for personal gain, such as running commercial businesses or engaging in unauthorised online activities is prohibited.

Personal Device Use

- Personal devices may only be used for College purposes with prior permission and under specific guidelines determined by the College from time to time. A consent form may have to be signed prior to being granted permission to use a personal device, containing an agreement to comply with the specific guidelines and this policy.
- Users are responsible for the security and appropriate use of their personal devices on College premises. The College assumes no responsibility for their loss, theft, or damage.
- Personal device use must not disrupt the learning environment or interfere with College activities.
- Personal devices must not be used to access websites or content prohibited on school technology.
- Recording audio or video with personal devices during school-related activities without the express consent of all individuals involved and in contravention to relevant laws and school policies is strictly prohibited.
- Users must not utilise personal email accounts and platforms for College-related communication or storage of school documents.

Use of School Identity

- PBC's name, or any images where PBC or PBC students are identifiable, such as students in uniform, may not be used as content to post online without the express permission of the College. This includes but is not limited to posting images or video footage on social media sites.
- Use of social media must not impact the reputation of PBC, or any previous/current PBC staff or students.

CONSEQUENCES OF VIOLATION

- PBC takes violations of this policy seriously. Misuse of ICT may result in a range of consequences, depending on the severity of the offence.
- Possible consequences may include:
    - Discussions: In some cases, violations may be addressed through discussions about acceptable use with the individual(s) involved and, if appropriate, parents or guardians.
    - Access Restrictions: The school may temporarily or permanently revoke a user's access to the network or limit their access to devices to ensure the safety and security of the school's digital environment.
    - Disciplinary Actions: For more serious violations, the school may take disciplinary actions, such as warnings, suspensions, expulsion, or termination of employment, in accordance with established disciplinary procedures.
    - Legal Consequences: Serious violations that involve illegal activities may also have legal consequences, including potential criminal charges.
- Users must report suspected violations of this policy promptly to Head of College or IT Support.

RESOURCES AND SUPPORT

- PBC will ensure that appropriate information, training, instruction, and supervision is provided to users to enable them to use PBC's ICT assets in accordance with this policy.
- For technical assistance, users may contact IT Support