ICT Use (Staff) Policy

1.Purpose

The purpose of this ICT Use (Staff) Policy is to establish clear expectations with staff regarding the use Information and Communication Technology (ICT) resources to ensure the protection, safety, and wellbeing of students, the broader school community, and the College's reputation.

Definitions

- ICT Resources: Includes computers, laptops, tablets, phones, internet services, email accounts, applications, storage devices, and any other technology owned or operated by My College.
- Professional Communication: Communication that maintains respect, appropriate boundaries, and protects the dignity and wellbeing of students and the broader community.

2.Scope

This policy applies to all staff members, contractors, volunteers, and any other authorised users accessing My College's ICT systems, networks, and resources, whether onsite or remotely. .

3.Policy Statement

My College is committed to promoting a safe, respectful, and professional environment in all aspects of school life, including the use of digital technologies.

4.Implementation

Appropriate Use of ICT Resources

- Staff must use College ICT resources in a professional, ethical, and lawful manner at all times.
- ICT resources must primarily be used for educational, administrative, and operational purposes related to College activities.
- Personal use must be minimal and must not interfere with work duties or breach College policies.

Professional Communication with Students

- Staff must maintain professional boundaries in all online communications with students.
- Staff must not engage with students via personal social media accounts, private messaging apps, or private email addresses.
- All communication with students must occur through authorised College platforms (e.g., Compass) and be directly related to educational or wellbeing matters.
- Staff must report any inappropriate communication initiated by a student immediately to leadership.

Privacy and Protection of Student Information

- Staff must not collect, use, share, or publish student photographs, videos, or personal information without checking that appropriate parental consent has been recorded on Compass.
- All handling of student information must comply with privacy legislation and the College's privacy policies.
- Storage and transfer of student information must be conducted securely.

Cybersecurity Responsibilities

- Staff must maintain the security of College ICT systems, including keeping passwords confidential and secure.
- Staff are responsible for ensuring that devices remain protected against unauthorised access or data loss.
- Any suspected cybersecurity breach must be reported immediately to the College's ICT Manager or Principal.

Monitoring and Auditing

- The College reserves the right to monitor, audit, and access staff use of ICT resources to ensure compliance with this policy and broader legal obligations.
- Staff acknowledge that there is no right to privacy when using College-provided ICT systems.

Prohibited Conduct

Staff must not:

- Access, store, create, transmit, or distribute material that is illegal, offensive, obscene, harassing, or discriminatory.
- Engage in grooming, exploitation, or any boundary violations through ICT systems.
- Use College ICT resources for personal financial gain, unauthorised commercial activities, or political advocacy unrelated to the College.
- Intentionally damage College ICT equipment or systems, or install unauthorised software.
- Access another user's account or data without explicit permission.

Breaches of this Policy

Breaches of this policy will be treated seriously and may result in disciplinary action, including but not limited to:

- Formal warnings;
- Restriction of access to College ICT resources;
- Suspension or termination of employment;
- Referral to external authorities where illegal activities are suspected.

5.Policy Review

Approved by: Principal and School Board, April 2025
Next review: April 2027