Acceptable use of digital technologies in Toowoomba Catholic Schools policy

Rationale

This policy sets expectations for safe, responsible and lawful use of Toowoomba Catholic Schools' (TCS) digital technologies (software, applications, networks, web pages, accounts, devices and online services). It supports teaching and learning, protects student wellbeing and child safety, protects staff, safeguards privacy and information security and maintains the integrity and availability of TCS systems.

To whom it applies

This policy applies to all users of TCS ICT digital technologies, including students, staff, contractors, volunteers, pre-service teachers and visitors, whether using TCS-owned or personally owned devices to access TCS systems. It applies on campus, during school activities (including camps and excursions) and, where there is a relevant connection to TCS, when using TCS accounts or services offsite.

Guiding principles

- Online safety and student wellbeing are paramount in all online environments.
- Digital technologies are used primarily for learning, teaching and legitimate TCS operations.
- Users act lawfully, ethically and respectfully (including in digital communication and online conduct).
- Privacy, confidentiality, information security, consent and recordkeeping obligations are upheld.
- TCS uses reasonable safeguards (including filtering, supervision and monitoring) and responds promptly to incidents.
- Use of emerging technologies (including generative AI) is guided by transparency, safety, Catholic values, academic integrity and data protection.

References

- Education (Accreditation of Non-State Schools) Act 2017 (Qld) and Education (Accreditation of Non-State Schools) Regulation 2017 (Qld)
- Education (General Provisions) Act 2006 (Qld)
- Working with Children Check Act 2000 (Qld), formerly the Working with Children (Risk Management and Screening) Act 2000 (Qld)
- Privacy Act 1988 (Cth), Australian Privacy Principles and OAIC Australian Privacy Principles Guidelines
- Anti-Discrimination Act 1991 (Qld)
- Work Health and Safety Act 2011 (Qld) and Work Health and Safety Regulation 2011 (Qld).
- Copyright Act 1968 (Cth) and relevant licence or usage terms
- Classification (Publications, Films and Computer Games) Act 1995 (Cth), National Classification Code and classification guidelines
- Relevant TCS policies, procedures and guidelines, including
    - TCS Privacy policy
    - ICT in Catholic schools policy
    - TCS Generative AI guideline for schools
    - Student protection policy
    - Data breach response procedure
    - Disciplinary action procedure

- TCS Staff Code of Conduct
- TCSO Staff Handbook
- TCS Parent engagement charter
- TCS Parent code of conduct
- TCS Enrolment application procedures
- Critical incident management procedure

Policy statement

All users must use only approved or authorised digital technologies. They are only to be used in ways that are safe, lawful, ethical and consistent with the mission and values of Catholic education, TCS codes of conduct and student behavioural expectations. TCS may implement security controls, filtering and monitoring to protect students, staff and systems.

Actions

1. General expectations (all users)

a. Use digital technologies primarily for learning, teaching and legitimate TCS operations.
b. Be respectful and inclusive online: communicate respectfully, include others and support a safe environment free from bullying, harassment, threats, shaming and discrimination.
c. Ensure all content you share, request or store is safe, ethical, legal and suitable for the intended audience
d. Protect privacy and confidentiality: only access information you are authorised to access, only use it for the intended purpose and only share what you are allowed to share.
e. Use strong passwords/passphrases, keep them private, use multi-factor authentication where enabled and lock screens when unattended.
f. Use only your own assigned login credentials: keep your login private and use it only to identify yourself.
g. When using a shared or multi-user device, check whether another user is signed in. If someone else is signed in, check whether they are still using the system and/or sign them out. Sign in only with your own account and sign out when finished.
h. Treat digital communication as a permanent record and communicate respectfully eg email, messaging, Learning Management System comments, forums and social platforms.
i. Respect copyright and intellectual property: reference sources and comply with licence terms.
j. Report cyberbullying, unsafe content, grooming concerns, lost/stolen devices, scams/phishing, suspected malware, access permissions inconsistent with your position, and any suspected privacy or security incidents promptly.

2. Student expectations

a. Use devices and online services at the times and in the ways directed by school staff and aligned to behavioural expectations.
b. Photograph, film or record only with permission and only in appropriate areas, keeping private areas such as toilets and change rooms free from recording.
c. Keep your own and others' personal information private; use privacy settings and manage location services carefully.
d. Maintain academic integrity: submit your own work, acknowledge all sources and follow assessment rules, including requirements for permitted AI use.
e. Use networks, devices and accounts in accordance with filtering and security controls, and use only authorised VPNs, hotspots and access methods.

3. Staff expectations

a. Meet duty of care obligations by actively supervising student online activity where required and responding to risks promptly.
b. Maintain professional boundaries in digital communication with students ie use approved platforms; avoid private channels and personal accounts unless explicitly authorised.
c. Only use TCS approved systems to store and share TCS information (including student and staff information) and follow recordkeeping requirements.
d. Upload personal, sensitive or confidential information only to approved services configured for that purpose, including when using generative AI tools.
e. Follow procurement/approval procedures for digital tools (including privacy, security and age-appropriateness checks) before classroom use.

4. Generative AI and automated tools (all users)

a. Users must use Generative AI and automated tools in line with TCS requirements for learning, assessment and work tasks.
b. Enter or upload personal information about students, families or staff, or confidential TCS information, only into AI and automated tools that are approved and configured for that purpose.
c. Be transparent: where AI is permitted, acknowledge its use in line with teacher/school expectations.
d. Check accuracy and bias: AI and automated tools output may be incorrect or inappropriate; users remain responsible for what they create, share or rely on.
e. Comply with copyright and licensing conditions for AI-generated and AI-assisted content.

5. Personal devices (all users)

a. Users may connect personal devices to TCS systems in accordance with TCS requirements (including configuration, updates, security software and acceptable use).
b. New and emerging personal devices must meet ICT and school standards and always be used in ethical, transparent and appropriate ways, in accordance with the TCS staff Code of Conduct and school's student behaviour support plans.
c. TCS may restrict access for non-compliant devices or require steps to protect the TCS network eg removing unauthorised software, disabling VPNs or applying security settings.
d. Personal devices may be used to record, store or share student or staff information only when explicitly authorised, provided appropriate security and protection measures are in place.
e. Lost, stolen or compromised devices used to access TCS accounts must be reported (see 7.) immediately so access can be secured.

6. Monitoring, filtering and privacy

a. To protect students, staff and TCS systems, TCS applies security controls (including web filtering), logs activity and monitors use of TCS networks, devices and accounts. This may be used for student wellbeing, security, misconduct investigations and legal compliance. Access to logs and content is restricted to authorised personnel and handled in accordance with privacy and recordkeeping obligations.

7. Reporting concerns and incidents

a. Students: tell a teacher, your pastoral care/wellbeing contact or a member of school leadership as soon as possible.
b. Staff/contractors/volunteers: notify your principal/line manager and the ICT/Information Services helpdesk (and follow any privacy, cyber security and the student protection reporting processes).
c. If there is an immediate risk to safety, contact the principal/line manager urgently and follow emergency procedures.
d. Report harmful content immediately without forwarding it. Preserve evidence by taking a screenshot where appropriate and safe to do so.

8. Breaches and consequences

a. Breaches of this policy may result in withdrawal of access to digital services, behavioural consequences for students, disciplinary action for staff (up to and including termination), and/or referral to external agencies (including police or regulators) where required. TCS will respond proportionately, with a focus on student safety and wellbeing, procedural fairness and legal obligations.

b. The requirements and recommended conduct described in this policy provide practical direction for the use of digital technologies, systems, devices and resources. Users are expected to act with caution, apply the guiding principles of this policy, and seek guidance from their principal, line manager, teacher (students only) or Information Services Service Desk if they are unsure about appropriate use.

Authority

This policy is the responsibility of the Director: Finance, Infrastructure and Information Services. Changes to this policy can only be made with the approval of the Director: Finance, Infrastructure and Information Services or the Executive Director: Catholic Schools.

Version control and change history

Effective date

16/10/2026

First published

28/10/2018

Republished

21/03/2025
4/09/2025
3/11/2025

Review date

16/10/2029