Diocese of Toowoomba
Catholic Schools

Acceptable Use of Toowoomba Catholic Schools provided Information and Communication Technology (ICT) systems, devices and resources policy (AUP)

Rationale

The provision of ICT systems, devices and resources by Toowoomba Catholic Schools (TCS) is to improve and enhance learning and teaching and the conduct of the business functions of TCS. Using information technology, information, and communicating electronically should be cost-effective, timely and efficient. To reap these benefits, it is essential that access to the appropriate use of these ICT systems, devices and resources be described and managed.

Legislative references

- Education (Accreditation of Non-State Schools) Act 2001 (Qld)
- Education (Accreditation of Non-State Schools) Regulation 2001 (Qld)
- Education (General Provisions) Act 2006 (Qld)
- Education (General Provisions) Regulation 2006 (Qld)
- Education (Queensland College of Teachers) Act 2005(Qld)
- Commission for Children and Young People and Child Guardian Act 2000 (Qld)
- Anti-Discrimination Act 1991 (Qld)
- Evidence Act 1977 (Qld)
- Work, Health and Safety Act 2011 (Qld)
- Work, Health and Safety Regulation 2011 (Qld)
- The Privacy Act 1988 (Commonwealth)
- Copyright Act 1968 (Commonwealth)
- Publications, Films and Computer Games Act 1995 (Commonwealth)

Policy statement

All employees and students (users) of TCS must access and use approved ICT systems, device and resources that meet agreed Information Systems standard, and in ways that are legal, ethical and are consistent with the purpose, mission, and values of Catholic education.

Actions

1. **Ownership and work-related use**
   a. TCS is the owner of all data, electronic communications created, sent, or received using TCS ICT systems, devices and resources. This includes school purchased devices and resources and access to the system from personally owned devices including laptops, mobile phones, tablets, or similar products.

b. Access and use of TCS ICT systems and resources includes
   i. publishing and browsing on the internet (during and outside of work hours)
   ii. downloading or accessing files from the internet or other electronic sources
   iii. email (inbox, sent items, folders and archives)
   iv. electronic bulletins/notice boards
   v. electronic discussion/news groups
   vi. weblogs ('blogs')
   vii. social networking
   viii. file transfer
   ix. file storage
   x. file sharing
   xi. video conferencing
   xii. streaming media
   xiii. instant messaging
   xiv. online discussion groups and 'chat' facilities
   xv. subscriptions to list servers, mailing lists or other like services
   xvi. copying, saving, or distributing files
   xvii. viewing material electronically and
   xviii. printing material.
   xix. accessing digital tools
   xx. artificial intelligence and subsets of artificial intelligence, such as but not limited to
      - deep learning
      - machine learning
      - large language models
      - small language models
      - agentic artificial intelligence.

c. All access and use of the TCS ICT systems, data, devices and resources (see 1.b.) will be monitored. Accordingly, all access including personally owned devices can be scrutinised at the request of the Chief Information Officer, school principal, an employee's supervisor, or legal authority including the police and courts.
d. Social networking, online conferences, discussion groups or other similar software services or tools using TCS ICT systems, device and resources must be relevant and used only for educational or business-related purposes. When using such tools, all TCS ICT users must conduct themselves in accordance with the TCS Employee Code of Conduct and/or the school's student behaviour requirements.
e. Electronic communications should be treated in the same way as any other correspondence, such as a letter; that is, as a permanent written record which may be read by persons other than the addressee, and which could result in personal or TCS liability.
f. Users and/or TCS may be liable for what is said in an email message. Electronic communications are neither private nor secret. They can be easily copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation.
g. Users should use the TCS ICT systems and resources responsibly and ethically. This includes
   i. treating all individuals with respect and dignity, regardless of sex, race, religion, national origin, or other characteristics
   ii. ensuring that all materials sent, received, accessed, downloaded, or distributed are appropriate and lawful
   iii. making comments that are suitable for the workplace environment
   iv. upholding the reputation of Toowoomba Catholic Schools Office and its schools

v. using email and messaging systems appropriately, avoiding spam, mass mail and chain mail
vi. respecting the copyright and intellectual property rights of others
vii. engaging in lawful and appropriate activities at all times.

h. Users of TCS ICT systems, devices and resources who receive unsolicited offensive or inappropriate material electronically should immediately report this to the Chief Information Officer, their supervisor, teacher or principal, and then delete it. Offensive or inappropriate material received from people known to the receiver should be deleted immediately and the sender of the material should be asked to refrain from sending such material again. Such material must not be forwarded internally or externally or saved onto TCS ICT systems, devices and resources except where the material is required for the purposes of investigating a breach of this policy.

2. Data Security

a. All diocesan\school data is owned by TCS and, as such, all users are responsible for appropriately respecting and protecting all data.
b. Users must only access data provided to them for duties in connection with their employment, education or engagement and in accordance with their terms and conditions of employment, enrolment or equivalent.
c. Users must only use personal information for purposes outlined in TCS Privacy Policy.
d. Extraction, manipulation, and reporting of TCS data must be done for TCS administrative and educational purposes only.
e. Personal use of TCS data, including derived data, in any format and at any location, is prohibited.

3. Privacy

a. While carrying out a user's duties on behalf of TCS, a user who has access to, or may handle personal information relating to others, including students, colleagues, contractors, parents/legal guardians and suppliers should not disclose this information except in accordance with TCS Privacy policy.
b. Each user is responsible for ensuring the security of ICT equipment provided for work and education purposes. Users should ensure that only authorised individuals, specifically employees or students of the TCS, use this equipment.
c. Users will be assigned a log-in code and will select a password to use on TCS's ICT systems, devices and resources. Each user must ensure that these log-in and password details are kept secure and private.
d. Users should either lock their screen or log-out when they leave their desk or complete a session of use.
e. When travelling overseas, users who require access to TCS ICT systems are to notify the Information Services Service Desk by lodging a support ticket or contacting support@twb.catholic.edu.au at least two weeks prior to travel.
f. To comply with TCS obligations under the Privacy Act (1988), users are required to use the blind copy (BCC) option when sending emails to multiple recipients where disclosure of those persons' email addresses will impinge upon their privacy.
g. In addition to the above, users are to familiarise themselves with the Australian Privacy Principles and ensure that their use of electronic communications complies with the Privacy Act (1988) or the Australian Privacy Principles.

4. Confidentiality

a. When electronic communications are sent from TCS ICT systems, devices, and resources to the network then on to the Internet, the communication may become public information. Encryption of emails should be used to reduce the risk of third parties being able to read emails and should be used in cases where additional security is required.

Please note: Receivers of encrypted emails require appropriate software to be able to decrypt them. If users require more information in relation to encrypting email, they should contact the

Information Services Service Desk - Toowoomba Catholic Schools Office via support@twb.catholic.edu.au.

b. Users must be aware that security of electronic communications is not guaranteed, particularly when communicated to an external party. The sender should consider the confidentiality of the material they intend to send and choose the most appropriate means of communication.

   Please note: There is always a trail and a saved copy of electronic communications on TCS ICT systems, along with other servers to which the communications pass. This applies even when encryption is used.

c. Where an outgoing email is important or urgent, users should verify that the recipient has received the entire email including any attachments.

d. All emails that are sent from TCS email addresses must contain the disclaimer message as shown below.

   The contents of this email are confidential. Any unauthorised use of the contents is expressly prohibited. If you have received this email in error, please advise the sender by email or telephone +61 7 4687 4321 immediately and then delete/destroy the email and any printed copies. Thank you.

   Please note: This message is set to appear automatically on each outgoing email. Contact the Information Services Service Desk via support@twb.catholic.edu.au if this feature is not working.

e. Users should maintain a reasonable degree of caution regarding the identity of the sender of incoming messages and verify the identity of the sender by another means if they have concerns.

f. Users must delete old or unnecessary email messages, sent, and deleted emails, and archive only those emails they need to keep. Emails that will be required for later review are to be saved in a confidential network folder, or if appropriate, in a shared folder to ensure that backups are made.

5. Distribution and copyright

a. All materials that are created, stored, and distributed using TCS ICT systems, and resources become the property of the TCS, unless they have been reproduced, with permission, in accordance with copyright laws, from a third party.

b. When distributing information over the TCS computer network or to third parties outside TCS, a user must ensure that TCS has the right to do so, and that they are respecting the intellectual property rights of any third party.

c. If a user is unsure of whether they have the sufficient authorisation to distribute the information, they are to contact their immediate supervisor, principal or information services for guidance.

d. Copyright law must always be observed. The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files and downloaded information) can only be distributed through TCS systems with specific authorisation to do so.

6. Viruses and malware

a. All external files and attachments are virus checked using scanning software before they are accessed.

b. Virus and malware checking is done automatically through protection software installed on TCS information technology infrastructure and devices.

c. If users are concerned about an email attachment or believe that it has not been automatically scanned for viruses, they should contact the Information Services Service Desk at support@twb.catholic.edu.au.

d. Only attachments from known and trusted sources should be opened.

7. Absence

a. During periods of absence from work or school, arrangements must be made to enable access to a user's email by TCS or an 'out of office reply' must be set.

b. If a user requires assistance with installing an 'out of office' reply, they are to contact the Information Services Service Desk at support@twb.catholic.edu.au.

c. At any time, the Executive Director: Catholic Schools, Directors or Principals can request access to another users emails through the Chief Information Officer, who will direct the Information Services Service Desk at support@twb.catholic.edu.au to facilitate the request where arrangements described in 6.a. and 6.b. have not been made.

8. Storage of devices and equipment

a. All ICT devices and equipment provided by TCS for staff and student use are to be stored in an area or place with a minimal possibility of theft or damage.

9. Breaches of this Policy

a. Depending on the nature of the inappropriate use of TCS ICT systems and resources, non-compliance with this policy may constitute
   i. a breach of employment obligations (staff)
   ii. a breach of the enrolment agreement (students and parents/legal guardians)
   iii. serious misconduct
   iv. sexual harassment
   v. unlawful discrimination
   vi. a criminal offence
   vii. a threat to the security of TCS ICT systems and resources
   viii. an infringement of the privacy of staff and other persons, or
   ix. exposure to legal liability.

b. Non-compliance with this policy will be investigated and appropriate action, including disciplinary action or termination of employment for staff and formal behaviour sanctions for students, will be taken.

c. Where there is a reasonable belief that illegal activity may have occurred TCS will report the suspected illegal activity to the police.

d. Examples of breaches of this policy include but are not limited to the following.

   i. **Category 1: Criminal**

      This category includes the following.

      - child abuse and child exploitation material
      - copyright violations
      - material showing intent to commit fraud
      - computer Crime
      - other - any other material or activity which involves or is in furtherance of a breach of the criminal law

   ii. **Category 2: Extreme**

      This category involves use of material that has or would attract a classification of RC under the Guidelines for Classification of Films and Computer Games 2005, or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth). This covers any material that

      - depicts, expresses, or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should not be classified
      - describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not), or
      - promotes, incites, or instructs in matters of crime or violence.

      This category also includes use of other types of offensive material that

      - has or would attract a classification of X18+ under Guidelines for Classification of Films

and Computer Games 2005 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth). The material covered by this classification is only available for hire or sale in the ACT and Northern Territory, and covers sexually explicit material that contains real depictions of actual sexual intercourse and other sexual activity between consenting adults

- involves racial or religious vilification
- is unlawfully discriminatory
- is defamatory
- involves sexual harassment; or
- brings or has the potential to bring the employee and/or the TCS into disrepute.

iii. **Category 3: Moderate**

This category includes the following.

- language that would be considered offensive or discriminatory under the Code
- depictions of violence that depicts the act of moderate physical or emotional harm
- partial or full nudity including cartoon nudity which does not show genitalia

iv. **Category 4: Low**

This category includes the following.

- content that includes occasional text or verbal language that would be considered offensive or discriminatory under the Code
- content that contains photographic, audio or text that would depict threatening or aggressive behaviour or low level physical or emotional harm

This category also covers personal use which satisfies the following 3 criteria.

- it occurs during normal working hours (but excluding the employee's lunch or other official breaks); and
- it adversely affects, or could reasonably be expected to adversely affect the performance of the employee's duties; and
- the use is more than insignificant.

10. Policy updates

This policy may be updated or revised from time to time. TCS will notify users each time the policy is changed via established communication methods. If users are unsure whether they are reading the most current version, refer to the TCS website.

11. General

The terms and recommended conduct described in this Policy are not intended to be exhaustive, nor do they anticipate every possible use of TCS ICT systems, devices and resources. Users are encouraged to act with caution and take into account the underlying principles intended by this Policy. If users feel unsure of appropriate action relating to use of ICT systems and resources, they should contact the Information Services Service Desk at support@twb.catholic.edu.au.

Authority

This Acceptable Use of Toowoomba Catholic Schools provided ICT systems and resources policy (AUP). is the responsibility of the Director: Finance, Infrastructure and Information Services (FIIS). Any changes to this policy can only be made with the approval of the Director: FIIS or the Executive Director: Catholic Schools.

Version control and change history

Effective date	First published	Republished	Review date
3/11/2025	28/10/2018	21/03/2025 4/09/2025	3/10/2028