Catholic Education
Diocese of Rockhampton

Information and Communications Technologies Code of Practice

Student
Primary Years 3 – 6

Version 8 • December 2023
Document Number: D17/31347[V8]
Date of next Review: 2024
Author: Administration

Contents

L

1. Introduction

The purpose of Information and Communications Technologies (ICT) at St Paul's Catholic Primary School is to:

- enhance student learning opportunities;
- promote student achievement;
- support student – school communication;

The use of ICT within schools should be safe, responsible, legal, appropriate and for educational purposes and should follow the guidelines outlined in this Code of Practice.

This ICT Code of Practice applies to the use of all school related ICT for educational purposes, whether provided by the school or the student.

Both students and parents/guardians must read and sign this ICT Code of Practice. It should then be returned to your class teacher, or submitted electronically via TASS Parent Lounge or Student Café.

2. Definitions

The following words are commonly used within this Code of Practice and are defined as follows to assist you in reading this document:

"**Catholic Education**" means The Roman Catholic Trust Corporation for the Diocese of Rockhampton trading as Catholic Education – Diocese of Rockhampton (CEDR). Catholic Education – Diocese of Rockhampton includes the Catholic Education Office (CEO), Catholic systemic schools, services, and work sites of Catholic Education – Diocese of Rockhampton.

"**Student**" means persons enrolled within a Catholic Education school within the Diocese of Rockhampton.

"**Information and Communications Technologies**" (ICT) means any electronic devices or services which allow users to process, record, send or receive information, in digital, audio, text, image or video form. These devices or services may include but are not restricted to standalone and networked:

- computer systems and related applications such as email and internet;
- social media;
- mobile devices including wearable technologies;
- communication equipment;
- output devices such as printers;
- imaging tools such as video or still cameras;
- audio tools such as audio recording devices;

- software applications and externally provided electronic services.

"**Social media**" means websites, applications, and any other service or device which enable a user to create and share content or to participate in social networking. This includes but is not limited to Facebook, LinkedIn, Instagram, Snapchat, Pinterest, TikTok, Discord, Twitter, blogs, forums, discussion boards, chat rooms, wikis, and YouTube.

3. Acceptable Uses

3.1 Students should:

- Respect resources.
- Use ICT equipment and resources for educational purposes under adult supervision.
- Follow teacher directions for accessing files, programs, email and internet resources.
- Ask permission from the teacher before following online prompts.
- Respect self and others by:
    - Respecting the rights, beliefs and viewpoints of others.
    - Following the same standards of behaviour online as one is expected to follow in real life.
    - Observing copyright rules by respecting the information, ideas and artistic works of others by acknowledging the author or publisher of information from the internet and not claiming the work or pictures as your own.
- Keep safe online by:
    - Keeping passwords and personal work secure. If it is suspected that a password has been compromised, steps must be taken to change the password immediately.
    - Using the internet and email for educational purposes.
    - Using school email accounts, not personal accounts, when communicating online at school.
    - Using social media appropriately including abiding by the application's terms and conditions.
    - Being cyber safe and embracing the principles of good digital citizenship.

4. Unacceptable Uses

4.1 Respect others

Online communications sent using the school's ICT will be recorded and monitored.

You should NOT:

- Post or send inappropriate, hurtful or inaccurate comments about another person.
- Use disrespectful or inappropriate language.
- Harass or bully another person. If someone tells you to stop sending them messages, you must stop.
- Take or send emails, photos, sound or video recordings of people without their permission
- Add your teacher or other school staff as friends or contacts on social media platforms.
- Use the ideas or writings of others and present them as if they were your own.
- Use the passwords or access the files of other users.
- Contact or communicate with teaching or non-teaching staff via personal email addresses or messaging platforms.

4.2 Keeping yourself safe

You should NOT:

- Send photos or post detailed personal information about yourself or other people. (Personal contact information includes your full name, date of birth / age, home address, telephone or mobile number, school address, email addresses, etc.).
- Use internet social networks, online chats, discussion groups or mailing lists that are not relevant to your education.
- Provide your password to others.
- Download files or share files with other internet users without teacher permission.
- Attempt to bypass the school's network security.
- Access personal mobile phones or wearable technologies during school hours.

4.3 Illegal Activities

Students need to be aware that they are subject to laws which prohibit posting, receiving or forwarding of illegal material, including those governing bullying, trafficking and computer offences.

5. Notification

You should:

- Tell your teacher or parent/guardian immediately about any messages you receive that are rude or that upset or worry you.
- Report inappropriate communications using the application's reporting mechanisms.
- Tell a teacher or parent/guardian immediately if you accidentally access something inappropriate.
- Tell a teacher or parent/guardian if someone else is doing something which offends you or is not permitted.

This will make sure that you are not blamed for deliberately breaking the School's ICT Code of Practice.

6. Consequences of Improper and Unacceptable Use

Minor breaches of the ICT Code of Practice will be addressed by the relevant <School name> staff member in line with <school's name> behaviour management procedures. If deemed inappropriate, the student's account may be suspended.

Ongoing or serious breaches of the ICT Code of Practice may result in further consequences, including suspension and / or exclusion from the school.

Please note, all schools and colleges in the Diocese of Rockhampton are legally required to pass on information to police relating to the possession, distribution or production of child exploitation material.

In summary, consequences for any student breaking these rules may include:

- loss of access privileges for a period of time;
- informing parents/guardians;
- suspension or termination of enrolment;
- legal action;

7. Cloud Services for Education – Advice for Parents

7.1 All students have access to educational collaborative Virtual Learning Environments (VLE), Google Workspace for Education and Microsoft 365. These environments provide access to email and a range of collaborative and productivity tools.

7.2 In using the Virtual Learning Environment provided through CEnet and Catholic Education Diocese of Rockhampton (CEDR), students (with parent permission) consent to the transfer, processing and storage of their data within cloud services.

7.3 The agreements with Google and Microsoft and the actions taken by the Diocese to establish ICT Codes of Practice will ensure the protection of personal information in accordance with national privacy, data usage, and data security guidelines.

- All advertising is disabled for education users to ensure that there is no tracking of school emails or web browsing.
- All mail is automatically scanned to perform spam filtering, virus detection and to block inappropriate content.
- Both Microsoft and Google maintain data centres in Australia, however some components of these services may be hosted outside Australia.
- Authorised staff within Catholic Education will have the ability to access, monitor, and audit emails and associated data as well as internet sites visited for the purposes of managing the system and ensuring its proper use.