Catholic Education
Diocese of Rockhampton

# Information and Communications Technologies Code of Practice

## Student
## Secondary Years 7 – 12

Version 8 • December 2023
Document Number: D17/31348[V8]
Date of next Review: 2024
Author: Administration

# Contents

# 1. Introduction

The purpose of Information and Communications Technologies (ICT) for students at **<….insert school name here….>** is to:

- enhance student learning opportunities;
- promote student achievement;
- educate our students to be safe and responsible users of digital technologies;
- raise awareness of issues such as online privacy, intellectual property, and copyright;
- support student – school communication;

The use of ICT within the school should be safe, responsible, legal, and appropriate 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 whether provided by the school, employees of the school, or the student.

Both students and parents/guardians must read this ICT Code of Practice. It will then be accepted via TASS Parent Lounge and Student Café.

# 2. Definitions

The following words are commonly used within this *ICT 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 includes the Catholic Education Office (CEO), Catholic systemic schools, services and work sites of Catholic Education.

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

"**Information and Communications Technologies**" (ICT) means any electronic devices or services which allow users to record, send or receive information, in 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 networking sites
- blogs, micro-blogs, forums, discussion boards and groups
- mobile devices including phones and wearable technologies;
- communication and networking equipment;
- output devices such as printers;
- imaging tools such as video or still cameras;
- audio tools such as audio recording devices;
- software applications/apps and externally provided electronic services.

"**Social media**" means websites and 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, Tik Tok, Twitter, Mastodon, blogs, forums, discussion boards, chat rooms, wikis and YouTube.

# 3. Acceptable Uses

Students should:

- Respect resources.
- Use ICT equipment and resources for educational purposes independently and under adult supervision.
- Access files, programs, email and internet resources appropriately.
- 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 offline;
  - 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.
  - This also includes content generated by products such as ChatGPT and Google Bard (and other generative AI tools)
- Keep safe by:
  - Ensuring passwords and personal work are secure. If it is suspected that a password has been compromised, steps must be taken to change the password immediately.
  - Using school email accounts, not personal accounts, when communicating for educational purposes.
  - Using social media appropriately including abiding by the application's terms and conditions.
  - Embracing the principles of good digital citizenship.

# 4. Unacceptable Uses

### 4.1 Personal Safety

Disclosure of personal information can expose users to inappropriate material, physical danger, unsolicited commercial material, financial risks, harassment and bullying, exploitation, unreliable information, nuisance, and sabotage.

You should NOT:

- Send or post detailed personal information, images or audio about yourself or other people. Personal contact information includes your full name, date of birth / age, home address, telephone or mobile number, school address or work address.
- Publish email addresses to public sites.
- Access personal mobile phones or wearable technologies during school hours.

### 4.2 Respect for Privacy

You should NOT:

- Distribute private information, including email, photos or recordings, about another person without their permission.
- Take photos, sound or video recordings of people, including background figures and voices, without their permission or as part of an approved lesson.

### 4.3 Respect for Others

You should NOT:

- Make personal attacks including harassing and bullying another person. If someone tells you to stop sending them messages, you must comply with their request.
- Send or post any inappropriate or inaccurate information, comments, images, video or audio about other people, the school or other organisations.
- Send or post personal information about other people without their permission.
- Contact or communicate with teaching or non-teaching staff via personal email addresses or messaging platforms.

### 4.4 Inappropriate Language

Restrictions against 'inappropriate language' apply to public messages, private messages, and material posted on web pages.

Messages sent using the school's ICT are recorded, monitored and scanned.

You should NOT:

- Use obscene, profane, rude, threatening, sexist, racist, disrespectful, or inappropriate language.

### 4.5 Access to Inappropriate Material

Attempts to access inappropriate material using the school's ICT is monitored and logged by the school or the Catholic Education Office.

Some inappropriate material may be filtered or blocked by CEDR, however we acknowledge that full protection from inappropriate content can never be guaranteed.

You should NOT:

- Use ICT to access material that:
  - is profane or obscene (e.g. pornography);
  - advocates illegal acts;
  - advocates violence or discrimination towards other people;
- Participate in internet social networks, online chats, discussion groups or mailing lists that are not relevant to your education.
- Access material which is not relevant to your education.
- Use the school ICT to purchase, order or sell any goods.

### 4.6 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.

An electronic audit trail may provide evidence of offences.

You should NOT:

- Attempt to gain access to any computer system or service, to which you do not have authorised access. This includes attempting to log in through another person's account or accessing another person's files or emails.
- Make deliberate attempts to disrupt other people's use of ICT.
- Make deliberate attempts to destroy data by hacking, spreading computer viruses or by any other means.
- Engage in any illegal acts.
- Install or use software on school owned devices which is not authorised by the school.

### 4.7 Plagiarism and Copyright

You should NOT:

- Plagiarise works found on the internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
- Use material from the internet in a manner which violates copyright laws.
- Access or use material from the internet which relates to exam cheating or providing completed assignments.
- This also includes content generated by products such as ChatGPT and Google Bard (and other generative AI tools)

### 4.8 Network Security

You should NOT:

- Provide your password to another person.
- Go looking for network security access, because this may be seen as an attempt to gain unauthorised access to the network.
- Post information that, if acted upon, could cause damage to, or disrupt the network.
- Open e-mails from unknown sources.
- Attempt to bypass the security settings of the school network or computing devices.
- Install or utilise software or technology e.g. VPN, anonymisers, or hotspots which bypass the school or CEDR filters or security systems.

### 4.9 Respecting Resource Limits

You should NOT:

- Post or respond to chain letters or engage in 'spamming'. Spamming is sending an annoying or unnecessary message to a large number of people.

# 5. Notification

You should:

- Report inappropriate communications using the application's reporting mechanisms.
- Notify the teacher or a carer if you identify a possible security problem.
- Immediately disclose accidental access to inappropriate material to your teacher. This will protect you against an allegation that you have intentionally violated the School's ICT Code of Practice.
- Notify the teacher if you are offended by another person's use of ICT.
- Tell a teacher or parent/guardian if someone else is doing something which offends you or is not permitted.

# 6. Consequences of Improper Use

Minor breaches of the *ICT Code of Practice* will be addressed by the relevant staff member in line with our schools 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 college.

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 sexual abuse material, images or video of themselves or their peers, including that which has been taken or shared consensually. The outcome of the investigation conducted by police will impact on the consequences to the student/s by the college.

In summary, any user violation will be recorded and may be subject to the following consequences:

- 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) which include 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 Environments provided through CEDR, students (with parent/guardian 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 CEDR 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.

- While connected to the CEDR network, internet traffic is scanned by Web Content Filtering technology.
- 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.

# Information and Communications Technologies Code of Practice

## Letter of Agreement

***Student***

I understand and will abide by this *ICT Code of Practice*. I further understand that any violation of the above is unethical and may constitute a criminal offence. Should I commit any violation, my access privileges may be revoked and disciplinary and/or legal action may be taken.

Name (Please Print): _____

**Signature:** _____ **Date:** _____

***Parent or Caregiver***

As the parent or caregiver of this student, I have read the *ICT Code of Practice*. I understand that these resources are designed for educational purposes. I also recognise that it is not always possible to completely restrict access to inappropriate material, even with Web Content Filtering systems in place.

I hereby give permission for my child to be given access to information and communication technologies as deemed appropriate by the school. I am also aware that ICT Cloud service providers used by the Diocese may transfer, store and process data outside Australia.

Name (Please Print): _____

**Signature:** _____ **Date:** _____

**NOTE: Failure to accept this agreement to your school will result in loss of access to ICT. Please respond and approve this access via TASS Parent Lounge. There is no need to return the paper form.**