Catholic Education
Diocese of Rockhampton

Information and Communications Technologies Code of Practice

Staff

Version 2 • January 2018

Contents

1. Scope

This Information and Communications Technologies (ICT) Code of Practice applies to all staff employed by Catholic Education Diocese of Rockhampton who use ICT resources and services, regardless of where or when those resources and services are accessed.

2. Rationale

The use of ICT resources and services is essential to Catholic Education's mission of providing outstanding quality education. In support of this objective, Catholic Education provides staff with access to ICT resources and services. In order to ensure the integrity, security and availability of ICT resources; staff must ensure that ICT is used only in a professional and responsible manner. The intention of this Code of Practice is to promote good decision making and encourage responsible use of ICT.

3. Statement

This ICT Code of Practice is intended to operate within, and be consistent with, existing State and Commonwealth Legislation and Catholic Education policies. It is intended to encourage responsible action, reduce risk attached to the use of ICT resources and services and to protect privacy.

Sanctions will be enforced if you act irresponsibly and disregard your obligations to other users, or to Catholic Education as the provider of ICT resources and services. Inappropriate use of resources and services used within Catholic Education may also result in warnings, suspension, termination of employment, legal action, or other disciplinary action.

4. Definitions

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

A. "**Staff**" means persons employed by Catholic Education. This includes persons employed on a full-time, part-time, temporary, permanent, contractual, casual basis or through an agency.

   This term also includes volunteers, student teachers and any other adults who in the course of their duties, have access to school or office owned or administered ICT in schools, the Catholic Education Office (CEO) and any associated work sites.

B. "**Information and Communications Technologies**" 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:

i. computer systems and related applications/apps such as email and internet;

ii. social media;

iii. mobile devices;

iv. communication equipment;

v. output devices such as printers;

vi. imaging tools such as video or still cameras;

vii. audio tools such as audio recording devices;

viii. software applications/apps and externally provided electronic services.

App: Software designed for a single purpose and performs a single function
Application: Software designed to perform a variety of functions.

C. "**Social media**" means websites and applications/apps 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, Omegle, Twitter, blogs, forums, discussion boards, chat rooms, Wikis and YouTube.

D. "**Catholic Education**" means The Roman Catholic Trust Corporation for the Diocese of Rockhampton trading as Catholic Education - Diocese of Rockhampton. Catholic Education includes the Catholic Education Office (CEO), its associated work sites and Catholic systemic schools in the Diocese of Rockhampton;

E. "**Personal information**" as defined by the *Privacy Act* 1988 is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not, and whether recorded in a material form or not. This includes photographs, video and audio recordings, report card comments, contact information etc.

F. "**Sensitive information**" means the definition provided by the *Privacy Act* 1988 and is information or opinion about an individual's racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; criminal record or health information about an individual. Sensitive information is subject to the personal information control rules and further rules as detailed in the Catholic Education Privacy Policy.

5. Procedures

5.1 Authorised access

A. Use and access to ICT resources and services is provisioned conditionally to those with proper authorisation and in accordance with each staff member's role.

B. Responsibility and accountability for ICT security is the shared responsibility of all users. You will be held responsible for all activities which originate from

your account. It is your responsibility to ensure that your passwords, accounts, software and data are adequately secured.

C. Subscriptions to applications/apps or services where content is shared with internal/external communities must have prior school leadership consent and access including administrative control.

D. If you know or suspect that another person has gained unauthorised access to your account, you must immediately notify your supervisor.

5.2 Training

A. Each staff member is responsible for ensuring that they are familiar with this Code of Practice and any other rules governing the use of ICT in each school, service or CEO.

B. Staff will be in-serviced and sign a statement of compliance with this ICT Code of Practice at commencement of employment and each school year thereafter. This Code will be updated from time to time and staff will receive a notification from CEO or their supervisor at that time. Staff have a responsibility to ensure that they read and understand any changes.

5.3 Enforcement

A. Enforcement of this Code of Practice will be the responsibility of:

i. Within each school or OSHC; the Principal.

ii. Within each kindergarten; the Early Learning and Care Coordinator.

iii. Within each region; the Assistant Director – Schools for the region.

iv. Within the Catholic Education Office; the Director.

B. This code is maintained and reviewed by the leadership team.

C. Guidance on the application of this code or breaches of this code can be sought from your supervisor.

5.4 Monitoring

A. The use of Catholic Education ICT resources and services is monitored, recorded and audited.

B. Electronic filters and monitoring systems may additionally report any unacceptable or unauthorised uses to authorised personnel within Catholic Education for attention.

C. Emails and other forms of communications should be considered insecure as they are difficult to destroy. Content may be retransmitted and accessed beyond the original intended recipients or purpose.

6. Uses

6.1 Acceptable Uses

A. Use of ICT resources and services is acceptable and encouraged where the use:

i. Is lawful;

ii. Is for the purpose of fulfilling an employment obligation such as:
    - Administrative functions; or
    - Furthering the educational objectives of Catholic Education.

iii. Supports the goals and objectives of Catholic Education.

iv. Is not an unacceptable use;

v. Does not breach other parts of this Code of Practice or other School or Diocesan policies or Codes of Practice;

vi. Does not adversely impact on employment performance;

6.2 Unacceptable Uses

The following are unacceptable uses of ICT:

A. Any use in breach of Diocesan or school policies, codes of conduct or procedures.

B. Any use with a direct or indirect purpose to discriminate, vilify, defame, harass, or bully.

C. Any attempts to intentionally injure the reputation of or cause embarrassment to Catholic Education.

D. Any illegal use.

E. Posting information that could cause damage or a danger of disruption of normal working and study conditions within Catholic Education.

F. Attempts to access or disseminate material or use language which is illegal, profane, obscene, threatening or inflammatory including material containing illegal acts, gambling, unlawful discrimination towards others, violence, hate, horror or pornography.

G. Any use of Catholic Education ICT for the conduct of business other than official Catholic Education business.

H. Engaging in inappropriate activities, including, but not restricted to "spamming" (sending an annoying or unnecessary message to a large number of people), "hacking" (attempting unauthorised access to a system or service), disseminating chain emails, inappropriate or offensive emails.

I. Use of ICT in such a way as to impede the access or efficiency of other users.

J. Communicating information concerning any password, identifying code or other confidential information, except in relation to legitimate work related duties.

K. Accessing, handling or using personal information or sensitive information (see definitions section of this Code for more information about what is classed as personal information and sensitive information) for a purpose other than that for which the information was collected. Staff must at all times ensure compliance with the Catholic Education Privacy Policy.

L. Excessive personal use of ICT resources and services including excessive printing or excessive personal internet use.

M. Use of ICT resources and services for a fraudulent purpose, for example, emailing views or opinions in your employment capacity without actually being authorised to express those views or opinions on behalf of Catholic Education.

N. The use of school or Catholic Education intellectual property, trademarks, copyright images and logos for any use other than for that which is approved by the School or Catholic Education.

6.2 Specific Notes on Unacceptable Use

A. If staff wish to use ICT resources and services for a use which is classified as unacceptable in this document, staff can only do so on the basis that access has a clear and direct link to fulfilling employment obligations (for example: investigating unacceptable use reports, researching gambling for class lesson plans). Before accessing such sites, staff must at all times, be prepared to provide evidence to link the use to the staff member's employment obligations. Staff must seek written consent from a member of the leadership team prior to undertaking the unacceptable use.

B. Electronic communications such as email, text message and published comments on public and personal online forums can easily be misconstrued. Staff should ensure that communications are published using clear and professional language to avoid misinterpretation.

C. Software (licensed, shareware, freeware etc) including application/apps, system and data files should only be downloaded in accordance with workplace instructions. The aim is to reduce the risk of hacking, overloading ICT resources and services and ensuring a uniform ICT system throughout each individual system.

D. If staff receive material which involves an unacceptable use, it must be reported to the Leadership Team for advice before being deleted.

7. Personal Use

The CEO recognises that staff may require the use of ICT resources and services for family and personal reasons. Such personal use must:

A. Be reasonable;

B. Be brief;

C. Not interfere with the performance of work;

D. Be otherwise subject to all the requirements of school and Catholic Education policies and this ICT Code of Practice.

8. Social Media

8.1 Overview

Guiding principles for the use of social media are:

i. Online behaviour should at all times demonstrate a Christ-centred respect for the dignity of each person;

ii. The Student Protection Policy of Catholic Education Diocese of Rockhampton must always be observed;

iii. Staff and student online interaction must occur only in an educational context;

iv. Staff must behave in an ethical manner when interacting and using online community sites, resources and services.

v. Staff are required to engage with Catholic Education's Social Media Framework.

8.2 Purpose

The purpose of this section is to encourage acceptable use of social media by staff employed by Catholic Education. The intent here is to assist staff to choose appropriate online activities for use with students and to maintain professional standards in each staff member's own use of social media.

8.2 Aim

The aim is to provide guidance to staff to ensure appropriate use of social media and to prevent instances of:

i. Possession, distribution or production of child exploitation material;

ii. Harassment, bullying or discrimination;

iii. Inappropriate or offensive comments;

iv. Privacy breaches;

v. Illegal uses or uses which infringe on the rights of others.

8.4 The Public Nature of Social Media

The use of social media is not without risk. Staff should be aware of the following:

i. Staff are accountable for their online communications which are work-related or made using Catholic Education ICT resources and services.

ii. Staff have an ability to serve as a positive role model for students. As a representative of Catholic Education, this is a critical aspect of their employment;

iii. Social media activities may be visible to current, past or prospective students, parents, colleagues and community members.

iv. Staff must exercise discretion when using social media (even for personal communication) particularly when those communications may reflect on their role within Catholic Education;

v. Social media publications have the potential to become public (even if posted in "private" forums). Consequently, publications on social media should be made using professional and clear language. Staff should publish social media publications as though the publication were to be read by the entire community.

vi. Staff should be aware of and understand the nature of the power imbalance between staff and student. All staff must act in a manner that always respects and never exploits the power inherent in these relationships.

8.5 Work related use of social media:

A. Publication of Information

i. Staff are required to handle sensitive and personal information relating to people who interact with Catholic Education (including students, staff, contractors, volunteers etc) in accordance with the Catholic Education Privacy Policy.

ii. Staff must not use commentary deemed to be defamatory, obscene, proprietary or libellous. Staff are to exercise caution with regards to exaggeration, colourful language, guesswork, copyrighted materials, legal conclusions and derogatory remarks or characterisations.

B. Online Learning Communities

i. If a staff member requests a student to register and use an online learning community (as part of the student's curriculum), staff should seek informed consent from the student and from the student's parents. In giving the consent, students and parents need to be made aware of:

- The name of online community;
- Brief description and, terms and conditions of the online community;
- Whether or not Catholic Education controls or can monitor usage of the student's participation in the online community;
- Any other matter which might be relevant under any other Policy (including the Privacy Policy).

Staff must ensure that prior to using the online community, students are educated in and made aware of the ICT Code of Practice – Students.

ii. Staff must provide students with clear instruction about their responsibility for appropriate interaction with others and suitable content posting online. Students should be taught about the appropriate use of social media within the context of cyber-safety education and responsible digital citizenry and how to report any attacks or inappropriate content.

8.6 Personal use of Social Media

Staff can reduce the risk of negative publicity and legal action and protect themselves and Catholic Education by observing the following guidelines with regard to the personal use of social media:

A. Social media, in a personal use context and not directly linked to the employee's role in the school, must not be used as a learning or communication tool for students.

B. Staff must not accept students presently enrolled in any school as “friends” or connections on their own social networks or interact with students on social media. The only exception to this is immediate family. This is for the protection of students and staff.

C. Staff are advised to use professional discretion before accepting or inviting ex-students or parents of current students as friends via social media.

D. Staff must not discuss students or co-workers or publicly criticise the school or Catholic Education policies or personnel on social media.

E. Staff must not post images that include students, other than immediate family, on personal social media.

F. Staff should give a high level of consideration to the appropriateness of posting personal comments online that may encroach on work issues. All comments of a private nature should not identify your school or be able to link staff to a school.

G. It is advisable to discuss with personal friends the need for discretion when they post images or information about you on their own social networks.

H. In no case should use of social media interfere with or impede an employee’s duties or responsibilities to the school or students.

I. Staff should ensure that they use social media both in a personal or professional context to represent the Catholic workplace well and not to use social media to bring themselves or their employer into disrepute.

J. Staff should ensure that privacy settings, where applicable, are set to a very high level. This is for the protection of staff and students.

9. Legal Requirements

9.1 Copyright, Plagiarism and Intellectual Property

A. Catholic Education is the copyright owner of all material created by staff in the course of fulfilling their employment obligations.

B. Staff must not use ICT resources and services to infringe the intellectual property rights belonging to Catholic Education or other parties;

Staff must not use intellectual property belonging to another person or entity unless the staff member has obtained the express consent of that person or entity or unless in accordance with an exception listed under the *Copyright Act* 1968 (Cth). If staff are unsure if the consent or authorisation applies to their proposed use, staff should seek instruction from their supervisor.

9.2 Legal Status of Information in ICT

A. All information stored in and transmitted on ICT must not be used contrary to the law, including anti-discrimination, privacy, child protection, defamation, bullying and sexual harassment legislation.

B. Electronically stored and transmitted documents (which include email, audio, image and video files) on CEO ICT devices are “discoverable documents” and may be subpoenaed in relation to Court proceedings and may be required to be disclosed.

9.3 Minimising Risk - ICT use

A. Catholic Education ICT access is electronically filtered with an end to block prohibited, obscene or illegal materials. Breaches of this filter, whether accidental or deliberate, should be immediately reported to your supervisor and then to ICT management.

B. Staff are to supervise student use of ICT resources and services with the goal of reducing the risk of harm suffered by students as a result of the use. Staff are required to take reasonable steps to:

   i. Ensure that students access the internet in accordance with the **ICT Code of Practice – Students**.

   ii. Provide an adequate system of supervision to the students as determined in accordance with risk management protocols;

   iii. Ensure safe and suitable premises and access location (such as school resources on school premises);

   iv. Implement strategies to prevent bullying including cyber-bullying (refer to Catholic Education Anti-Bullying Policy);

   v. Ensure that student access is for a purpose directly related to furthering the student's educational objectives in accordance with the student's set curriculum.

9.4 Privacy

A. The Catholic Education Privacy Policy sets out how Catholic Education collects, handles, uses, stores and discloses personal information and confidential information. All staff are required to be familiar and ensure that they comply with that Policy.

B. Personal information and sensitive information stored on ICT is password protected and access is determined by role. For more information on password protection guidelines, please see Item 9.6 of this Code.

C. Staff are responsible for ensuring the security of ICT resources and services to which they have access. This includes measures such as:

   i. Electronically locking a computer before leaving the workstation;

   ii. Only using secure internet connections;

   iii. Ensuring that materials downloaded or received from a source external to Catholic Education are filtered;

   iv. Not permitting anyone other than the user to access their account;

D. Personal and sensitive information should not be disclosed unless the disclosure is for the purpose for which the information is collected or the owner of the personal information consents to the disclosure. Personal information includes email addresses. Therefore, staff should use the blind copy option "BCC" when sending an email to multiple recipients to avoid infringing a person's right to privacy;

E. Staff should report any ICT security breaches to their supervisor.

9.5 Emails

A. Emails are filtered and monitored via spam, virus and language filters. Staff should be aware that ICT management and supervisors do have access to the school email network. Consequently, language in emails should be professional and work-related.

B. The Catholic Education Disclaimer is added automatically to all outbound email for services managed by Catholic Education. Staff should confirm with their principal or systems administrator the application of the disclaimer for all other email services. The following is the Catholic Education Office Disclaimer:

> *The information contained in the above e-mail message or messages which includes any attachment, is confidential and may be legally privileged. It is intended only for the use of the person or entity to which it is addressed. If you are not the addressee, any form of disclosure, copying, modification, distribution or any action taken or omitted in reliance on the information is unauthorised. Opinions contained in the message(s) do not necessarily reflect the opinions of the Catholic Education Diocese of Rockhampton. If you received this e-mail message in error, please immediately notify the sender and delete the message from your computer.*

C. If staff receive unwanted, inappropriate or offensive emails these should be reported immediately to your supervisor. Spam or hoax emails should be reported to ICT management.

9.6 Passwords

Staff have a responsibility for ensuring the security of passwords used to access ICT resources and services. The objective is to prevent unauthorised use and access to ICT resources and services. Staff passwords should be maintained as follows:

i. Are changed regularly (at least every 90 days).

ii. Use different passwords for different systems.

iii. Are confidential to the user.

10. Code of Practice Breach

10.1 Reporting

A. Staff have a responsibility to disclose any inadvertent or accidental unacceptable use of ICT resources and services to the Principal or designated supervisor. Such disclosure may protect staff in the event of an allegation that they have intentionally violated this Code of Practice.

B. Staff have a responsibility to report to the Principal or designated supervisor any unacceptable use of ICT resources and services by staff or students.

C. Usage of ICT resources and services is recorded and has the capacity to be monitored and investigated.

10.2 Processing

A. The unit supervisors within CEO and the Principal within each school are responsible for ensuring that staff are aware of and comply with this Code

of Practice. Those people are also responsible for processing any complaints or reports of breaches of this Code of Practice.

B. Whether the contravention of policy or Code of Practice entails internal disciplinary measures or attracts intervention from external bodies, the Catholic Education Office is committed to due process in any investigation and subsequent action.

C. All reports and complaints of breaches of this Code of Practice will be processed in accordance with the Catholic Education's Grievance Procedure Policy.

D. It may be appropriate, particularly in instances of illegal use of ICT or instances which might give rise to legal recourse, to seek legal advice. The Assistant Director: Schools in your school's region is the appropriate person to speak to regarding obtaining legal advice.

10.3 Consequences

A. Proven breaches of this Code of Practice, including social media, depending on the nature of the breach, may result in:

   i. Disciplinary action including a sanction, warning or suspension;

   ii. Termination of employment;

   iii. Notification to external agencies such as the Police and Queensland College of Teachers;

   iv. Legal action.

B. The Catholic Education Office and/or schools will cooperate fully with local, state or commonwealth investigators in any procedures concerning or relating to any illegal activities.

11. Cloud Services for Education – Advice for Staff

A. All staff and students have access to educational collaborative Virtual Learning Environments (VLE) which are supported by CEnet and the diocese. These VLE are G-Suite for Education and Office 365, which are contained within a hosted environment, providing security for student and staff data. These environments provide access to email and a range of collaborative and productivity tools.

B. Staff are advised that the following are not to be retained in "cloud" services - sensitive student information and health records, taxation records, employee records under applicable industrial legislation, workers' compensation records, occupational health records, school attendance records.

12. Further Information

For further explanation about any matter contained in this Code of Practice, please contact your immediate supervisor or the Principal. Principals may seek direction from the Assistant Director: Schools in the school's region.

13. Supporting Instruments

The following instruments were considered in the drafting of this document and should be considered at each review:

CCI Factsheet – Developing and Internet Usage Policy

Privacy Act 1988 (Cth)

Right to Information Act 2009 (Qld)

Information Privacy Act 2009 (Qld)

Copyright Act 1968 (Cth)

Anti-Discrimination Act 1991 (Qld)

Catholic Education Grievance Procedures Policy

Catholic Education Privacy Policy

Social Media Framework Nov 2013 - Joint Working Party of QCEC and IEUA-QNT.

14. Review

This Code of Practice will be reviewed on an annual basis.