Catholic Education
Diocese of Rockhampton

Information and Communications Technologies Code of Practice

Staff

Version 8 • December 2023
Document Number: D17/31474[v8]
Date of next Review: 2024
Author: Administration

Contents

1. Scope

This Information and Communications Technologies (ICT) Code of Practice applies to all staff employed by Catholic Education Diocese of Rockhampton (CEDR) 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:

- 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.

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, Twitter, TikTok, Mastodon, 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 (CEDR). Catholic Education includes the Catholic Education Office (CEO), Catholic systemic schools, services, and work sites 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 CEDR *Privacy Policy*.

g. **"Digital Media"** includes live-streaming, video, audio and images (digital and print).
"Live Streaming" technology allows people to watch, create and share content in real time. All that is needed to live stream is an internet enabled device, such as a smartphone, tablet or computer, and a platform to live stream from.

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. This may include the use of your corporate account, including your Microsoft corporate account or Google corporate account, to sign in to a Third Party application.

d. You must not allow another person to use your account, even with your knowledge or permission. 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, student Codes of Practice where applicable, and any other rules governing the use of ICT in each school, service or CEO.

b. Staff will complete an online mandatory training course at the beginning of each year or on commencement of employment. On completion an electronic badge will be issued indicating that compliance has been satisfied for the ICT Code of Practice. This Code will be updated yearly. If major changes occur during the year 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.
c. Staff may also be required to undertake regular and ongoing Security Awareness Training.

5.3 Enforcement

a. Enforcement of this Code of Practice will be the responsibility of:
    i. Within each school or Outside School Hours Care (OSHC) - the Principal.
    ii. Within each kindergarten - the Early Learning and Care Manager.
    iii. Within each region; the Assistant Director: Schools for the region.
    iv. Within the Catholic Education Office - the Diocesan Director Catholic Education.
b. This code is maintained and reviewed by the Catholic Education 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

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 Catholic Education 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 Catholic Education 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, 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.

6.3 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). Staff must seek written consent from a member of the school or office leadership team prior to undertaking the unacceptable use, and must be prepared to provide evidence to link the use to the staff member's employment obligations.
b. Electronic communications such as email, text messages 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, security, 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 CEDR *Student Protection policy* 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 CEDR *Video Conferencing Guidelines*.
vi. Staff are required to engage with CEDR *Livestreaming Guidelines for Schools*.

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.

8.3 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 CEDR *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 or Community Platforms

   i. If a staff member requests a student to register and use an online learning community as part of the student's curriculum or outside activity, 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 the 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 CEDR *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*.

   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.

c. Digital Media

One aspect of digital content is live streams. They can be either private or public therefore staff must always ensure discretion.

Private Platforms, including Zoom, Teams, and Google Meet, can require a registration to access the event.

- Some Public and Private Platforms do not require registration and are available to large numbers of people who may be able to respond to the stream through posting comments or emojis.

Staff must be diligent by giving due consideration to the following:

- The school reputation especially when live streaming as it is 'in the moment' which increases the risk of students acting on impulse.
- Personal Privacy as a person's image may feature in the media format. All images are considered personal information therefore *Australian Privacy Principles* apply. Media permissions for all parties concerned must be adhered to.
- Inappropriate comments, especially if the media format is open to the public with the ability to add comments.
- Digital footprints as errors may occur or personal details may be shared. In relation to a live stream, a viewer can record and post or share more widely.
- Copyright ensuring that any material displayed or broadcast is adhering to copyright laws.

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. Production of Copyright Materials
   a. **General rule** - At law, material created by employees of CEDR in the course of their employment, regardless of whether it is created using CEDR facilities or materials, or during normal working hours, will belong to CEDR. What constitutes the course of employment will be determined by the employee's position description and usual duties.
   b. **Exception** - An employee's employment contract may vary the default position of when copyright belongs to CEDR. The employment contract overrides the default position that exists at law. Employees may be required to sign additional documents vesting or assigning copyright to CEDR where that material was created by the employee using CEDR resources and during paid working hours. One example of when this may be necessary is if the employee is required to engage in a project or duties that are outside of their normal employment duties.
   c. **Created during work hours** - If any material was created using CEDR resources, or during paid working hours, then the onus is on the employee to demonstrate that it was not created in the course of employment. Employees should be aware that performing unauthorised non-work tasks during work hours may subject them to disciplinary proceedings. Where any uncertainty exists, staff are encouraged to discuss this with their supervisors.
   d. **Others** - Works by independent contractors and volunteers shall be owned in accordance with the written contract under which the work was created. CEDR shall ensure that there is a written contract for work by an independent contractor or volunteer specifying ownership. At law, unless a written contract specifies otherwise then independent contractors and volunteers will own copyright in everything that they create.
   e. **Dispute** - Any dispute between CEDR and its staff, contractors or volunteers, or between staff, or between contractors or between volunteers, on issues of copyright ownership shall be determined by the organisation's dispute resolution procedures. Such determination will be subject to the judgement of any court or tribunal.

b. Use of copyright material
   a. Staff and volunteers of CEDR are required to observe all applicable copyright laws and regulations.
   b. Use of CEDR ICT resources and services for a purpose which infringes copyright, whether it is copyright owned by CEDR or a third party, is expressly forbidden. Any person who commits such an infringement shall be personally liable under the *Copyright Act*. CEDR may also be found liable.
   c. CEDR staff may only use copyright material belonging to others:
      i. Where the copyright material has been specifically licensed by CEDR and approved for use by staff; or
      ii. The staff member has obtained a licence to use the copyright material or is permitted to use the copyright material without a licence at law. If a staff member wishes to take up this option, they must seek guidance from their supervisor as to how to carry out this process.
   d. Staff and volunteers of CEDR may use copyright material belonging to or licensed to CEDR only for the purposes of their work for CEDR. Where the material is used by CEDR under licence, staff and volunteers must act in accordance with that licence.

e. Staff and volunteers of CEDR may not reproduce, publish, distribute or adapt third party copyright material in the course of their work for CEDR without the authorisation of the copyright owner. Staff and volunteers may not download or reproduce text, photographs or illustrations found on the internet without authorisation of the copyright owner. This includes for use in internal or external newsletters, reports or presentations. All non-generic images and illustration should be sourced from and with the consent of the creator. Generic images may be obtained from a stock image supplier (e.g. Shutterstock or iStockphoto).

f. When reproducing or otherwise using third party copyright material, it cannot be assumed that just because something is on the internet that it is free for everybody to copy and use. This includes images on Facebook or photo sharing websites such as Flickr. Acknowledgement of source of the material does not overcome the need for authorisation; actual authorisation is still required.

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 CEDR 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 CEDR *Student 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 CEDR *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 with it 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. Many systems are now also protected by Multi-Factor Authentication (MFA) which provides an additional level above something you know (password) with something you have (MFA app or token).
d. 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.
e. 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.
f. 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 CEDR 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 CEDR. 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 emails should be deleted, and hoax emails should be reported to ICT management.
d. Bulk email communication to students and school community should only be done via Teacher Kiosk and/or TASS communication functionality. This ensures communication is logged and stored appropriately within the Student Information System.

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, or if there is a suspicion that a password has been compromised;
ii. Use different passwords for different systems: do not use the same password for corporate and personal accounts;
iii. Are confidential to the user.

Password protection suggestions to maintain password confidentiality:

i. Do not reveal passwords to anyone telephonically or electronically;
ii. Do not reveal your passwords to support people or superiors;
iii. Do not share passwords with family members;
iv. Do not reveal passwords to co-workers while you are out of the office or school for extended periods of time;
v. Do not share passwords with any co-workers, e.g. administrative secretaries; and
vi. Do not write down your password.

9.7 Multi-Factor Authentication

Multi-Factor Authentication (MFA) is an essential part of securing your Catholic Education – Diocese of Rockhampton (CEDR) account. What it means is that after you enter your username and password, you may be prompted to verify who you are via another means – namely the Okta Verify app on your mobile device. Basically, something you know (password) + something you have (phone with Okta Verify).

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 CEO 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 *Right Relationship – Parent and Student Grievance Policy and Procedure*.
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 Federal or State Police and Queensland College of Teachers;
    iv. Legal action.

b. The CEO 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 CEDR. These VLE include Google Workspace for Education and Microsoft 365, which are contained within hosted environments, 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 only approved cloud services for the storage of personal and sensitive information are the CEDR tenancies of Microsoft 365 (including Office, Outlook, SharePoint, OneDrive for Business, Teams), and Google Workspace for Education (including Gmail, Drive, Google Docs, Classroom). These approved third-party service providers to CEDR have cloud storage as a component of their service offering.

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 Documents

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

- CCI Factsheet – Developing an Internet Usage Policy
- Queensland Legislation
    - Privacy Act 1988 (Cth)
    - Right to Information Act 2009 (Qld)
    - Information Privacy Act 2009 (Qld)
    - Copyright Act 1968 (Cth)
    - Anti-Discrimination Act 1991 (Qld)
- CEDR Student Anti-Bullying policy
- CEDR Student Protection policy
- CEDR Right Relationships – Parent and Student Grievance policy
- CEDR Right Relationships – Parent and Student Grievance Procedures
- CEDR Privacy policy
- CEDR Guidelines for Teachers using Video Conferencing
- CEDR Livestreaming Guidelines for Schools

14. Review

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