Student ICT Code of Practice

Based on Catholic Education Diocese of Rockhampton ICT Code of Practice
Student (Secondary Years 7-12) Version 1.1 • October 2015

Contents

1. Introduction

The purpose of Information and Communication Technologies (ICT) for students at Emmaus College is to:

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

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

This 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 and sign this Code of Practice to receive a school laptop.

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 Rockhampton. Catholic Education includes the Diocesan Catholic Education Office (DCEO), Catholic systemic schools, services and work sites in the Diocese of Rockhampton.

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

"**Information and Communication 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 media.
- mobile devices.
- 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 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, Omegle, Twitter, blogs, forums, discussion boards, chat rooms, Wikis and YouTube.

3. Monitoring

Emmaus College reserves the right to monitor laptop, intranet, internet and network usage and to inspect email messages sent or received to:

- Identity inappropriate use.
- Protect system security.
- Maintain system performance.
- Protect the rights and property of Emmaus College.
- Determine compliance with School and Diocesan Policy.
- Determine compliance with State and Federal legislation and regulation.

4. Acceptable Uses

4.1 Students should:

- Respect resources.
- Use ICT equipment and resources for educational purposes independently and under staff 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 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.

5. Unacceptable Uses

5.1 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.
- Meet with someone you have met online without your parent's/guardian's approval and participation.

5.2 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.

5.3 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.

5.4 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.

5.5 Access to Inappropriate Material

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

Some inappropriate material may be filtered or blocked by the school or Diocesan Catholic Education Office.

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.

5.6 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.

5.7 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.

5.8 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.

5.9 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.

6. Notification

You should:

- Disclose to your teacher any messages you receive that are inappropriate or disturb you.
- Report inappropriate communications using the application's reporting mechanisms.
- Notify your teacher 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 your 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.

7. Consequences of Improper Use

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.

8. Google Apps for Education – Advice for Parents

8.1 All students in Rockhampton Catholic Education and 15 other Catholic Dioceses in QLD and NSW have access to a very powerful collection of educational tools - Google Apps for Education (**GAFE**).

8.2 All students have access to this collaborative Virtual Learning Environment (VLE) which includes:
- email,
- calendars,
- google documents,
- presentations,
- blogs,
- spreadsheets,
- forms,
- groups,
- sites,
- maps and
- video.

8.3 Catholic Education Rockhampton provides email, document creation and online storage for learning through the Google Apps for Education service.

- Emails, email account details and data may be transferred, stored and processed in the United States or any other country utilised by Google to provide the Google Apps services.
- In using the school's email system and Google Applications students (with parent permission) consent to the transfer, processing and storage of that information.

8.4 The CENet Agreement with Google and the actions taken by Dioceses 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.
- 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.