



Information Communication Technology (ICT) Acceptable Use Policy

Document Author	Digital Learning Services Manager
Department Owner	Technology Advisory Group
Approver	Principal
Date Approved	December 2020
Review Date	December 2023

Purpose



An Acceptable ICT Use Policy includes measures for the appropriate, effective and equitable use of the College's ICT network.

At Catholic Regional College Caroline Springs, we support the rights of all members of the school community to be provided with, and engage in, a safe, inclusive and supportive learning environment. This extends to the use of digital tools and online communities and is underpinned by our expectation of safe and responsible behaviour of all members of the school community.

At Catholic Regional College Caroline Springs, we:

- educate our students to be safe and responsible users of digital technologies;
- raise our students' awareness of issues such as online privacy, intellectual property and copyright;
- supervise and support students when using digital technologies within the classroom and establish clear protocols and procedures when working in online spaces. This includes reviewing and considering the safety and appropriateness of online tools and communities;
- provide a filtered internet service but acknowledge that full protection from inappropriate content can never be guaranteed.
- respond to issues or incidents that have the potential to impact on the wellbeing of our students including those reported through online services; and
- know that some online activities are illegal and as such we are required to report this to the appropriate authority/ies.

Scripture



[Psalm 25:21](#)

May integrity and uprightness protect me, because my hope, LORD, is in you.

Scope



This policy applies to all College students and staff, including teaching, non-teaching, permanent and temporary employees and contractors, and parents/carers that access the colleges ICT services.

Policy



Access

1. Access to the College's Information and Communication Technology (ICT) network is provided for staff, students and parents/carers as a tool for educational use and to support College activities. Access to this resource is a privilege which carries with it responsibilities, as outlined in this Policy.
2. Do not use the College's ICT network in any way that infringes on the rights or privacy of others, or which violates the College's Privacy and Non-Disclosure Policies, or for commercial purposes.
3. You should only access the College's ICT network, any computer or secure system within the College using your own username and password, or an authorised 'shared' account for approved applications.
4. You must stop accessing any aspect of the College's network when you cease to be part of the College community.

Security

5. Always keep your username and password secure and private – do not disclose your password to anyone.
6. Always log off or lock your computer before you move away from it.
7. Portable devices in your care (including loan equipment such as a loan MacBook, recording equipment, etc) must always be kept securely, or in your possession;
8. Do not attempt to circumvent or compromise network security;
9. If you become aware of a ICT breach eg; Security or Data related, you must immediately inform a member of the Leadership Team or ICT Team at the College on (03) 9217 8000.

Online Behaviour

10. Your behaviour online should reflect your behaviour offline or in person; treat others fairly and with common courtesy. The College ICT Network must not be used as a medium to bully, harass, threaten or intimidate other users.
11. If you experience harassment or bullying online, do not respond. Record the details and save any information you can. Students should contact their Homeroom Teacher or Year Level Leader and staff should contact a member of Leadership as soon as possible.
12. You should not intentionally access, modify, copy nor move other staff members' or students' personal files or settings.
13. Students should not intentionally modify, move nor delete shared files stored on the Network, and staff should only do so in accordance with their Position on Leadership.
14. You must not install nor store inappropriate, illegal or unlicensed software on College computers nor on the College Network.
15. You may only utilise the College Network to host or participate in game playing if it is directly related to the approved curriculum for your subject area, in compliance with the Additional Student Software Procedure, and has been approved by the Technology Advisory Group.
16. You should not allow other users direct access to your computer through file sharing; eg. device to device)

Internet Usage

17. Internet access at the College is provided for educational use and therefore personal use should be limited. The College's internet connection is filtered to prevent access to sites which are deemed inappropriate for College use.
18. Be conscious of the quantity of data you consume when accessing the internet, including for educational purposes and avoid unnecessary or excessive use.
19. You should exercise care when using the internet and must not seek to access or download inappropriate, offensive, discriminatory nor intimidating material. If you encounter such material, you should disclose to and notify a teacher, Homeroom teacher, Year Level Leader or member of Leadership immediately.
20. Intentionally accessing, storing or distributing material that is inappropriate, offensive, discriminatory or intimidating in nature, or which puts any member of the community at risk, may lead to disciplinary action. This may involve reporting the matter to police where State or Federal laws have been breached.
21. When obtaining information from the Internet, do not infringe the copyright of others by using the information without permission or acknowledgement of the copyright holder.
22. Always exercise caution when downloading files from the internet, as these may contain viruses, adware or spyware. Anti-virus software is provided on all College-supplied Computers, and you should scan your computer regularly to ensure that it is free from infections.
23. The College will not be responsible for any loss or liability incurred by you through your use of the internet.

Social Media Usage

24. Staff should only access Social Media during College hours for appropriate educational purposes including administering and monitoring the College's social media accounts
25. Students should only access social media at the College when permitted to by a teacher for appropriate educational purposes
26. Inappropriate personal use of Social Media includes but is not limited to the following:
 - disclosing confidential or proprietary information;
 - posting images of other people without their consent;
 - use of the College's intellectual property, College logos;;
 - infringement of the intellectual property rights of others;
 - making statements adversely affecting the College's interests or reputation;
 - criticising the College, students, parents, staff, community partners, and/or anyone associated with the College;
 - using defamatory, harassing, or disparaging language or images;
 - forwarding or posting content that violates the law (e.g. obscenity);
 - writing or commenting on content that would constitute a violation of any other rules, standards of conduct or requirements applicable to staff members;
 - staff initiating or accepting 'friend' requests with any current or past College students*
 - staff holding conversations with students of a personal nature

** An exception to this requirement is when prior approval for the connection has been obtained from the Principal on the basis that an employee and a student will appropriately interact within the valid context of a legitimate purpose (for example, both are family members/relatives or both are members of a community sporting team and interactions are purely for the purpose of participating in that sport.)*

Email Usage

27. Email carries the same legal status as a signed letter or memorandum. It is considered a formal means of communication and care should be taken when composing and sending email. Responsible use of the email system is based on common sense, common decency and civility, and should not be used when face-to-face communication would be more appropriate.
28. Do not send unsolicited emails to multiple recipients. The distribution of email should be limited to necessary recipients only; the need to send global ('All Staff') emails should be carefully considered and aligned with College distribution.
29. Do not distribute or forward 'spam', hoax or 'chain' emails.
30. The College recognises that some non-school-related email communication will occur, and does not desire to prohibit this, but such use should be limited so that this privilege is not abused.
31. The following disclaimer will automatically appear on all external email communications:

IMPORTANT! This email and any attachments may be confidential. If received in error, please contact us and delete all copies. Catholic Regional College Caroline Springs does not represent nor warrant that the attached files are free from computer viruses or other defects. The attached files are provided, and may only be used, on the basis that the user assumes all responsibility for any loss, damage or consequence resulting directly or indirectly from the use of the attached files, whether caused by the negligence of the sender or not. The liability of Catholic Regional College Caroline Springs is limited in any event to either the resupply of the attached files or the cost of having the attached files resupplied. Any representations or opinions expressed in this email are those of the individual sender, and not necessarily those of Catholic Regional College Caroline Springs.

Printing

32. Care and conservation should be paramount considerations with regard to the use of College printing facilities. You should keep printing to a minimum and consider the environment when using print facilities.
33. You should review documents on screen and students should submit work electronically where appropriate.

Monitoring

34. The College reserves the right to, at any time, and without prior notice, examine email messages, files stored on computers and in network locations, internet favourites, history and cache files, and other information stored on computers and on the network, for material or activity that would constitute a breach of this Policy.

Complaints

35. The College maintains a comprehensive Grievance and Complaint Policy available from our college website.

Definitions



Social Media: A group of online applications which includes, but is not limited to social networking sites, wikis, blogs, microblogs, video and audio sharing sites and message/discussion boards, instant messaging that allow any individual to easily access, share, discuss and publish content in a public forum.

Related Documents



Privacy Policy

Standard Collection Notice

Student MacBook Agreement

Code of Academic Integrity

Grievance and Complaint Policy