



Student Electronic Communications Code of Conduct and User Agreement

Dear Parents and Students,

Emmanuel Anglican College would like to offer your child access to electronic communications including the Internet. Students are able to communicate with other individuals, schools and organisations within Australia and around the world through the use of the Internet, email and other online services. We believe that such access is a vital component of preparing our students to live in the 21st century.

This Code of Conduct outlines the College's expectation of student behaviour when accessing electronic communications and the College's network. The Code of Conduct applies to use of College owned property and privately owned devices while being used on College grounds or attending College related events.

The College will accept the role of teaching your child the rights and responsibilities of being a sensible network citizen but believes the teaching of cybersafe and responsible online behaviour is best taught in partnership between home and College.

The students for their part must accept that with access comes personal responsibility. As you would realise when using the Internet, access to objectionable material or material of an adult nature is possible. This Code outlines the College's stance on access to such material. Even though the College will take every precaution to prevent such access, current technology does not allow us to prevent access completely. Parents/carers should be aware that the nature of the internet is such that full protection from inappropriate content can never be guaranteed. Steps have been taken through two separate firewalls to prevent students either intentionally or unintentionally accessing content that is deemed dangerous or inappropriate. Students must therefore take a degree of responsibility, as outlined in this Code of Conduct. The College will take a **"no tolerance"** approach to accessing such material. Penalties for improper use will be enforced. Some online activities are illegal and as such will be reported to police.

Please read this Code of Conduct carefully with your son/daughter before signing the User Agreement. The Agreement is to be signed by yourself and your son/daughter.

Please return the following Student Electronic Communications Code of Conduct and User Agreement to the students Class or Pastoral Care Teacher. This page advises us that you have read and understand the Electronic Communications Code of Conduct.

STUDENT ELECTRONIC COMMUNICATIONS CODE OF CONDUCT

1. Students are responsible for the proper use of the College's Electronic Communications system, which will be referred to as the system throughout this document. The use of the Internet is a privilege, not a right, and inappropriate use will result in the loss of this privilege.
2. Students must: -
 - (a) not publish any school related material onto the Internet without the express permission of a Teacher or relevant College staff member;
 - (b) not publish any private information onto the internet while on College grounds or attending College related events;
 - (c) protect the privacy of others and never post or forward private information about another person without their consent;
 - (d) only take photos and record sound or video when it is part of an approved lesson;
 - (e) seek permission from individuals involved before taking photos, recording sound or videoing them;
 - (f) seek appropriate (written) permission from individuals involved before publishing or sending photos, recorded sound or video to anyone else or to any online space;
 - (g) be respectful in the photos taken or video captured and never use these as a tool for bullying.
3. Students shall not submit, publish or display on the College's system any knowingly inaccurate and/or objectionable material.
4. Transmission of material, information or software in violation of any College policy, local state or Commonwealth law is prohibited.
5. The College reserves the right to:
 - (a) monitor a student's phone, tablet and computer screen during school hours or while attending College related events;
 - (b) examine the content of all of the College's email messages sent and received by a student;
 - (c) ask that draft email content be changed if deemed unacceptable;
 - (d) refuse to permit the transmission of email messages that are deemed unacceptable (e.g. using offensive or objectionable text or pictures);
 - (e) monitor the College's email, which must at all times reflect the ethos of the College;
 - (f) ensure all of the College's email must carry the correct name of the sender and is sent to intended recipients (not recipients who do not need to receive the email e.g. sending an email to all students), and
 - (g) access a student's User Account associated with any software or application licensed to the College, including the ability to access, monitor, use, modify, withhold or disclose any data available to the end user.
6. Forgery or attempted forgery of email sent from or to a College email account is unacceptable.

Attempts to read, delete, copy, or modify other College email accounts are prohibited.

7. System users will remove any software or application licensed to the College, including email, in accordance with licensing requirements and established retention guidelines. The College IT Department may suspend and/or delete access to any software or application licensed to the College, if not attended to by the system user.
8. Students must only download files they intend to use for educational purposes and must do so in accordance within the confines of copyright laws. Students may download material onto a personal storage device, which must conform to copyright rules and the College reserves the right to inspect any personal storage device used at the College.
9. Students may print material via a Networked printer after obtaining permission from the class teacher at the time.
10. Students will be instructed to save their files onto the College provided drive storage. All such drives and any other areas on the system remain the property of the College and, as such, may be checked by the College IT Department for inappropriate files and information.
11. Students are expected to abide by the general accepted rules of network etiquette. These include, but are not limited to, the following.
 - a) Be polite. Your conduct should not be abusive to others.
 - b) Use appropriate language. Do not swear, use vulgarities, or any other language deemed inappropriate.
 - c) Do not disclose your personal address or phone number. Do not reveal the personal addresses and/or phone numbers of fellow students or colleagues.
 - d) Illegal activities are strictly forbidden.
 - e) Email is not guaranteed to be private and may be intercepted or tracked.
 - f) Online activity (including emails, comments or posts) relating to or in support of illegal activities may be reported to the authorities.
 - g) Do not use the internet in any way that would disrupt network services for other users.
 - h) All communications and information accessible via the internet should be assumed to be private property.
12. Deliberate attempts to degrade or disrupt system performance with outside programs (e.g. hacking programs) or attempts to bypass software designed to protect the system and its users will be viewed as a violation of College policy and administrative regulations and may be viewed as criminal activity under applicable law. The College reserves the right to instruct students to pay costs involved in repairing damage caused by said activities and such conduct will result in the cancellation of system use privileges.
13. The endpoint antivirus software installed on all College supplied computers will automatically complete a virus check on downloaded files to avoid computer viruses. However the College cannot guarantee that all viruses will be detected. The College does not accept responsibility

for the downloading of viruses or other problems to computers not owned by the College. Parents should adopt a 'virus prevention policy' in respect to their home and work computers.

14. Students who identify a security problem on the College's system must notify the class teacher or the College IT Department at the time.
15. Vandalism or any malicious attempt to harm or destroy College equipment or materials, data of other users of the College's system or any of the agencies or other connected Networks is prohibited. The College reserves the right to instruct students to pay costs involved in repairing damage caused by said activities, and such conduct will result in the cancellation of system use privileges. Staff will follow the Student Management Policy.
16. Software files not belonging to the College or the student (including movies & music) may not be loaded or used on any College computer. Students shall not copy or load any software (or files), that would constitute a breach of the copyright conditions attached to that software and the use of that software.
17. Students may not modify the operating system of any College computer or attempt to bypass any systems that have been setup to protect the integrity of the system. Students may not knowingly access, tamper with, or change any Network configuration settings.
18. Students are strictly prohibited from using mobile hotspots, Virtual Private Networks (VPNs) or any other means of bypassing the College's network security systems.
19. Students may not access the system under a name other than their own or attempt to enter the system using another person's password. Passwords must be kept secure at all times.

Personal Devices

20. The College may allow access to its Network from a privately owned device on the following conditions:
 - (a) An EAC teacher or staff member approves of the use of the personal device.
 - (b) The user agrees to abide by this Code of Conduct.
 - (c) Insurance for privately owned devices will be the responsibility of the student. The College will not be liable for the loss or damage to any privately owned personal devices on College premises.
 - (d) The student agrees to allow the College to inspect any data storage devices, including hard drives, USB sticks etc, if deemed necessary.
 - (e) The personal device will be used only for educational or other approved purposes whilst at College.
 - (f) The personal devices must be charged prior to entering the classroom. No charging cords are to be connected in the classrooms.

- (g) Students would only be permitted to have one privately owned device on the College Network.
 - (h) The student's private device must have a purchased and up to date antivirus software installed. Integrated operating system security and other free antivirus software is not acceptable.
 - (i) If the student's private device does not have a purchased and up to date antivirus software installed, the College reserves the right to install antivirus on the private device using the College's site license.
21. Any student who does not conform to the Code of Conduct may have their system privileges revoked for a period of time. Consistent history of violations of the Code will lead to the denial of access to the system.

Printing

22. Print counting software is operating on our Network. Every student will be allocated a complementary amount of printing, depending upon his or her year level.

Lost Data

23. Students are advised to keep a backup of all data files that are not stored in a College Google Drive Folder. Loss of data (assignments) cannot be used as an excuse for late submission (see Parent/Student Guide and the College Planner).

Privacy

25. The College encourages an environment where students are assured that the privacy of their communications will be respected, as long as they abide by the College's Code of Conduct. The College reserves the right to monitor all areas of the Network including College owned devices, student College email, Internet searching, drive space supplied by the College and privately owned devices (including smart phones, laptop/notebook computers, iPads and iPods).

Disclaimer

26. The College does not warrant that the functions or services performed by or that the information or software contained on the system will meet the system users requirements or that the system will be uninterrupted or error free or that defects will be corrected. The College's system is provided on an "as is as available" basis. The College does not make any warranties, whether express or implied, including without limitation, those of merchant ability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein.

Student Electronic Communications User Agreement

Student Name (please print):	
Home Address:	

I understand and will abide by the Electronic Communications Code of Conduct. I further understand that any violation of the regulations is unethical and may constitute a criminal offence.

Student's Signature:
(Year 5 and above)

Date:

/ /

Parent or Guardian

As a parent or guardian of this student, I have read the terms and conditions for Network and Internet access. I understand that this access is designed for educational purposes. However, I also recognise it is impossible for Emmanuel Anglican College to restrict access to all controversial materials and I will not hold Emmanuel Anglican College responsible for materials acquired on the network. Further, I accept full responsibility if and when my child's use is not in a College setting. I hereby give my permission to grant access for my child and certify that the information on this form is correct.

Parent/ Guardian Signature:

Date:

/ /