



POL4.7 BYOD Code of Conduct

RATIONALE	<p>The BYOD Code of Conduct aims to provide an engaging learning environment in an eSafe (electronically safe) culture in keeping with the values of the College.</p> <p>The College provides you with the opportunity to use ICT equipment and devices and gives you rights to use and access services on the College network. The College expects you to act responsibly with all ICT equipment and facilities.</p>
SCOPE	This policy applies to all students and families of Trinity Lutheran College.
RESPONSIBILITY	The Principal has overall responsibility for this policy, which is administered with assistance of all teaching and IT staff.
DEFINITIONS	<ul style="list-style-type: none"> • 'eSafety' refers to the safe use of the internet and electronic communication systems. • 'Electronic communication' includes, but is not limited to communication made by using ICT equipment/devices such as Internet, Intranet, email and mobile phone activities and related applications. • 'ICT' the term 'Information and Communication Technologies'. • 'ICT equipment/devices' include, but is not limited to, computers (such as desktops, laptops/notebooks, ipads, PDA's), storage devices (such as USB and flash memory devices, CDs, DVDs, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other similar technologies as they come into use. • 'Agreement' means this Code of Conduct and any other similar agreement which may be developed by the College from time to time. • 'Prohibited use' means use of College ICT or privately owned or leased ICT on the College site or at any College-related activity, in a manner which is contrary to the terms of this Agreement. • 'College' means Trinity Lutheran College. • 'College related activity' includes, but is not limited to, an excursion, camp, sporting or cultural event, wherever its location. • 'Unacceptable use' includes, but is not limited to, acts of a malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, deliberate defacement or damage to any ICT device or equipment, plagiarism, gaming, impersonation/identity theft, inappropriate use of email.
POLICY	<p>1. Security</p> <p>1.1. For security reasons we expect students to keep passwords and network login details private. Students need to keep all drives and files secure, and prevent others from accessing work without permission. Students must respect the rights and privacy of others and under no condition access other students network accounts though their password and login, or through unacceptable use or illegal means, e.g. hacking.</p> <p>2. Storage</p> <p>2.1. Students are responsible for managing their own files.</p>



POLICY_POL4.7_BYOD Code of Conduct Policy

- 2.2. USB devices are accepted for school related resources/documents to be stored on. These are not to be used to transfer games or music to and from the College.

3. Internet

- 3.1. Internet access is provided to students for educational purposes. The College provides access to quality online information sources through a range of portals. The allowance made to students for Internet use is generous and appropriate for such educational usage.
- 3.2. Accessing online sites purely for personal use or entertainment (such as games) is a breach of this agreement. Students are to speak with their teacher or the ICT Support Officer about access if they are in doubt.
- 3.3. Use of file-sharing, torrents, VPN's, proxies are specifically banned and blocked by the College system. Students are not to use such services at school and should ensure they are disabled.
- 3.4. Access to the Internet via the College's facilities may not be used to browse, download or distribute material which is of an anti-social nature, pornographic, violent, illegal, racist, destructive, demeaning or denigrating of others or which encourages this. Students must respect laws and other people's rights, including copyright laws and antidiscrimination laws. Use of social networks (such as Facebook), public chat sites and programs are not permitted.
- 3.5. All use of the Internet is recorded and the Information Technology Department can monitor all Internet sites visited by students should there be cause for concern. Random monitoring of BYOD devices also takes place throughout the year.

4. Copyright

- 4.1. Copyright laws and licensing agreements must be respected and sources appropriately acknowledged and referenced. Students are expected to abide by the Copyright Laws and licensing agreements. The fair dealing legislation allows student use of copyrighted materials provided they abide by attribution and referencing of materials.

5. Network Printing & Internet Use

- 5.1. The College provides network printers for use at various locations around the school. A reasonable print allocation is provided. If this allocation is exceeded, the ability to print at school will be suspended until additional print capacity is purchased by the student at the Administration Office.

6. Email

- 6.1 If students are in years 5 to 10 you are also provided with a unique email address.
- 6.2 Students school email is only used in class time at the request of the class teacher or as required for school communication to you.
- 6.3 Use of public chat sites and programs is not permitted, unless agreed to by the class teacher. It should be noted that your email address carries the College name. Therefore, the email network must NEVER be used to make comments that are
- 6.3.1 rude, obscene or offensive, including discrimination against any person or group;
- 6.3.2 are discourteous to an individual or organisation;
- 6.3.3 might injure the reputation of another person or offend that person;



POLICY_POL4.7_BYOD Code of Conduct Policy

6.3.4 are trivial or likely to annoy the receiver.

7. BYOD Devices

- 7.1 Students are given permission to bring a device to the College. Students are required to agree to use the device only during class session and for classwork only.
- 7.2 Students will be personally responsible for preventing loss or damage to their device.

8. Privacy

- 8.1 The Privacy Act requires the College to take reasonable steps to protect the personal information that is held by the College from misuse and unauthorised access.
- 8.2 Whilst access to the ICT facilities is provided to you by way of a personal account, authorised members of the College ICT staff reserve the right to investigate the way students use the facilities including email and internet browsing.
- 8.3 It is understood that students will have personal information on their device. Students are expected to manage this entirely. The College bears no responsibility for the misuse or unauthorised access of these devices.
- 8.4 Personal hotspots and bypassing the Trinity internet filters and firewalls are specifically banned whilst students are at school.
- 8.5 While after school use of technology by students is the responsibility of parents, College policy requires that no student attending the College may identify, discuss, photograph or otherwise publish personal information or personal opinions about College staff, fellow students or the College. This also applies to College related activities.
- 8.6 The College takes a strong position to protect privacy and prevent personal information and opinions being published over technology networks including Facebook, Instagram, YouTube, Twitter, Snapchat (and any subsequent new technology and social media platforms).

9. eSafety

- 9.1 It is the responsibility of all students to be proactive to ensure their safety in online environments. The College provides education for students about cyber safety and other digital environment safety.
- 9.2 Students are expected to use all ICT equipment in an appropriate and safe way at all times on campus. This includes personal devices such as phones.

BREACH OF POLICY

Breaches of this agreement can undermine the values of the College and the safety of students, especially when ICT is used to facilitate misconduct. Such a breach deemed by the College to be harmful to the safety of the College or its members, may result in disciplinary action.

10. Consequences for Breaking the Code of Conduct

- 10.1 A warning will be given and, if need be, the teacher will make an infringement record notifying the parents and other staff.
- 10.2 Repeated or more serious infringements of BYOD Code could result in:
 - a. removal of internet access for a period
 - b. removal of the device for a period
 - c. suspension from the College



POLICY_POL4.7_BYOD Code of Conduct Policy

RELATED DOCUMENTS

- d. Police involvement
- 10.3 Any suspicion by College staff of inappropriate activity on the student's device related to child safety will be immediately reported to the appropriate authorities for investigation.

POL4.6_Bring Your Own Device (BYOD) Policy
 POL1.8_Student Code of Conduct Policy
 BYOD Program Years 5 to 10 Guide
 My BYOD Code of Conduct Agreement

RECORD OF IMPLEMENTATION

Contact officer	Eloise Beveridge (Principal)
Approved by	Executive leadership 12/10/2020
Ratified by	Trinity Lutheran College Council
Authorization	Trinity Lutheran College Council authorizes this policy for publication and implementation having considered relevant legislation and/or operational requirement of users.
Tracking	Ratified [DATE].
Review Date (3 year cycle or as required by legislation)	2022