TRINITY LUTHERAN COLLEGE

P-12 eSmart Policy for Students, Parents and College Staff

INTRODUCTION

Over the past two decades our lives have been transformed by a digital revolution. New devices and new technologies have enriched our lives but have also introduced new challenges.

The aim of this policy and eSmart Agreement is to support and encourage each member of our college community – students, parents, staff, volunteers, contractors and guests – in their safe, smart and responsible use of information communication technology.

Together, through education and shared responsibility, we can create an eSmart culture that promotes and values the online safety, privacy and wellbeing of each member of our Trinity Lutheran College community.

Relevant to: All students P-12, their parents, and all staff of the college.

Positions responsible:

ICT Manager; Head of Campus, Early & Junior Years; Head of Campus, Middle & Senior Years

Definitions of terms used in this policy and agreement

a. '**Agreement'** means this policy and the eSmart Agreement and any future amendments or revisions as deemed necessary by the college.

b. **'Appropriate use'** refers to the use of college owned or privately-owned information communication technologies (ICT) as outlined in the eSmart Policy.

c. **'College'** means Trinity Lutheran College.

d. **'College staff'** refers to teaching staff, non-teaching staff, volunteers and contractors.

e. **'College related activity'** includes but is not limited to excursions; camps; learning, sporting or cultural activities.

f. **'Communication technologies'** includes, but is not limited to, communication made using ICT equipment/devices such as internet, intranet, email, instant messaging, online discussions/surveys, mobile phone activities, and all related applications.

g. **'Cyberbullying'** is a form of bullying using communication technology. Bullying is anti-social conduct involving a pattern of uninvited, on-going behaviour directed by a more powerful person or group to intentionally or unintentionally hurt, injure, embarrass and/or distress a less powerful person or group. If there is no power imbalance, it is not considered bullying.

h. **'Digital citizenship'** is defined as the norms of safe, smart, responsible behaviour with regard to communication technology use.

i. **'Digital footprint"** refers to the combination of all online posts made by an individual.

j. **'Digital reputation'** is defined as a person's or organisation's behaviour in the online environment and by the content that the person posts about oneself and others.

k. **'Digital technologies'** is used to describe the use of digital resources to effectively find, analyse, create, communicate, and use information in a digital context. This encompasses the use of web 2.0 tools, digital media tools, programming tools and software applications.

l. **'Educational purposes'** means activities that are linked to curriculum related learning.

m. **'eLearning tools'** includes, but is not limited to, myUnity and any online applications and programs that are used for educational purposes.

n. **'eSmart'** refers to the safe, smart, responsible use of ICT.

o. **'ICT'** stands for 'Information and Communication Technologies' and includes network facilities, communication technologies, eLearning tools and ICT equipment/devices.

p. **'ICT equipment/devices'** include, but are not limited to, computers (such as desktops, laptops, tablets), storage devices (such as USB and flash memory devices, CDs, DVDs, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, and any other, similar, technologies as they come into use.

q. **'Member of our college community'** means a person who, by virtue of employment, enrolment contract, volunteering, tutoring, coaching or other contractual relationship, is obliged to abide by the policies of the College.

r. **'MyUnity'** is the college's learning content management system (LCMS) and communication portal.

s. **'Network facilities'** includes, but is not limited to, intranet and internet access to files, web sites and digital resources via the college wireless network.

t. **'Objectionable material'** deals with matters such as pornography, cruelty, violence, or material of a discriminatory nature that it is likely to be injurious to students and thereby incompatible with a college environment.

u. **'Unacceptable conduct'** includes, but is not limited to, malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, non-sanctioned gaming, impersonation/identity theft, copyright infringement, or cheating in an examination.

v. **'User'** means a person who, by virtue of employment, volunteering, enrolment contract or other contractual relationship, is obliged to abide by the policies of the college.

w. **'Parent** includes custodial guardian or caregiver.

x. **'Social media'** refers to online spaces that enable anyone to publish and access information. Social media includes (but is not limited to):
- social networking sites (e.g. Facebook, Instagram, LinkedIn, Bebo, Yammer) etc.
- video and photo sharing websites (e.g. Flickr, YouTube etc.)
- blogs, including corporate blogs and personal blogs
- micro-blogging (e.g. Twitter)
- wikis and online collaborations (e.g. Wikipedia)
- forum discussion boards and groups (e.g. Google groups)
- podcasting
- online multi-playing game formats (e.g. World of Warcraft)
- electronic messaging (e.g. emails, SMS)
- geo-spatial tagging (e.g. Foursquare)

USER ESMART OBLIGATIONS

1. Authorised usage and eSmart agreement

1.1. This policy and eSmart Agreement supersedes all previous agreements relating to information communication technology (ICT) used at Trinity Lutheran College. Any future amendments or revisions to this policy and Agreement will appear on the College website with immediate effect. The latest version is available for download from the college's parent portal.

1.2. To support and encourage the online safety and wellbeing of each member of our college community users are obliged to abide by the conditions of this policy and all related policies.

This is inclusive of college owned or personally owned information communication technology, including mobile phones, and regardless of access via our college server or via a third-party server beyond our college premises.

1.3. With online safety and wellbeing as our priority, the college therefore reserves the right to monitor individual usage on its server and report or delete any content

- that breaches the ethos, values and standards of our college or terms of agreement of online sites such as age restriction for apps and social media sites e.g. Facebook

- or is deemed unlawful.

2. User obligations and requirements regarding appropriate use of college ICT

2.1 As online safety and wellbeing is a whole of community concern, the behaviour of each member of our community should at all times reflect the highest standards of honesty, respect and consideration both in person and online, toward all persons and the college in general.

2.2 Each member of our college community is therefore personally responsible for comments, images and videos they publish online using college owned or personally owned communication technology when accessing the college server.

2.3 For one's own safety and the safety of others users should always act on the assumption that, even on the strictest privacy settings, all posts are in the public domain. This is particularly true when microblogging e.g. Twitter as such sites are not protected by privacy settings.

2.4 Similarly, users should not access or post any material that is in breach of S.474.17 of the Criminal Code, that is, material that is fraudulent, harassing, threatening, intimidating, pornographic, a breach of privacy, defamatory or otherwise inappropriate or unlawful, regardless of access via our college server or via a third-party server beyond our college premises.

Unacceptable conduct may also include that which:

- constitutes a contempt of court
- breaches a court suppression order
- fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus
- attempts to breach security and infrastructure that is in place to protect user safety and privacy
- represents an unauthorised external or internal access to the college's electronic communication and administration systems. This includes all 'blocked' or 'designated only' authorised user sites.
- inhibits the user's ability to perform his/her duties productively and without unnecessary interruption
- interferes with the ability of others to conduct the business of the college
- can be deemed as malicious activity resulting in deliberate damage to college ICT and/or ICT equipment/devices
- involves the installation and/or downloading of software which contravenes this policy.

2.5 In the event of accidental access of objectionable or unlawful content users are encouraged to:

- not show others
- shut down, close or minimise the window
- report the incident immediately to the supervising teacher or a member of the college administration.

3 Profiles and identity

3.1 A person's digital reputation is defined by a person's behaviour in the online environment and by the content posted about oneself and others. The online environment includes mobile phones.

3.2 Tagged photos, blog posts and social networking interactions all shape how a person is perceived by others, both online and offline, now and in the future.

3.3 For employees of the college, a person's digital reputation is also an extension of that individual's professional life.

3.4 One's personal reputation online is therefore something of value and should therefore be protected at all times.

3.5 Further, information posted or stored online, including images are permanent, becoming public by default. Users are encouraged to ensure all online posts, including those using mobile phones, are consistent with the ethos, values and standards or our college community and are lawful.

4 Individual password logons to user accounts

4.1 For access to our network it is necessary to obtain a personal user account from the college. Importantly, such login information allows the college to trace any inappropriate or unlawful use of our college's network and to respond with expediency.

4.2 Each time an individual adds something about oneself online, one increases his or her digital footprint. Whenever a person mentions someone else, we increase the mentioned person's footprint. Just as a person's digital reputation is something to value and protect, so too is one's online personal identity.

4.3 Each member of our college community is encouraged to ensure usernames and passwords always remain confidential. A breach of this requirement could lead to users being denied access to our college network.

4.4 Users are also encouraged to safeguard against the access by another person to any information communication technology, including mobile phones, logged in under their own user account. Material accessed on a user account is the responsibility of that user.

4.5 Where the device, including mobile phone, belongs to another student, the appropriate consequences for misuse may therefore also apply to the owner of that electronic device.

5 Privacy

5.1 The Privacy Act requires reasonable steps to be taken to protect the personal information of each member of our community that is held by the college from misuse or unauthorised access.

5.2 A person's right to privacy must be respected and protected at all times. Personal information may include, but is not limited to, home or email addresses, telephone numbers (including mobile phones), passwords, pin numbers.

As mentioned previously, each member of our college community should act on the assumption that all online posts are in the public domain.

5.3 Users should not post any identifying information including photographs and/or videos or personal opinions that may be perceived as defamatory about any member of our college community or the college in general.

5.4 Similarly, in-phone cameras on ICT devices, including mobile phones, should never be used anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets.

5.5 Where a member of our college community inadvertently discloses personal or confidential information, the matter is to be reported immediately to the relevant Head of Campus so the college may expedite steps to minimise any possible distress.

5.6 Further, where users inadvertently gain access, by whatever means, to a blocked college intranet site, the matter must be reported immediately to the relevant Head of Campus. Failure to report may unintentionally also cause distress to others and may constitute a breach of privacy and/or professional misconduct.

5.7 Legislative requirements such as those pertaining to Privacy, Intellectual Property, Copyright and Child Protection must always be observed.

For example, images of college buildings, buses, sports teams, school grounds, logos, staff or students in uniform etc. are the Intellectual Property of the college. Further, online publication of such material may place the privacy and safety of members of our college community at risk and therefore is prohibited by the college.

6 Copyright, intellectual property, licensing, and publication

6.1 Copyright, moral right or intellectual property laws, as well as licensing agreements must be respected, and sources appropriately acknowledged.

6.2 A hyperlink to outside sources is recommended. It also is recommended that blogs be licenced under a Creative Commons Licence.

6.3 All student written assessment is to be submitted electronically through myUnity. This is recommended from Year 8 and required from Year 10 onwards.

6.4 A student found using ICT, including mobile phones, to gain an advantage in a test or exam will face disciplinary actions in accordance with the college's Academic Policy.

6.5 In the classroom the use of digital devices, for example mobile phones and smart watches is at the discretion of the teacher. Information accessed including photos and music should be appropriate and conducive to the learning environment and legally procured.

7 Maintenance of professional boundaries of college employees including social media

7.1 Given the assumption that all online posts are in the public domain, reference to the college, the college's operations and/or college related matters are never to be discussed online with other colleagues, parents, or students.

7.2 When employees comment in a professional capacity, on the college's operations or a college related matter or member/s of our community there is the potential for damage to be caused, either directly or indirectly, to those members and/or our college community as a whole via the personal use of social media.

To protect our community and all of its valued members, users who are college employees are authorised to comment on behalf of the college only in respect of matters approved in writing by the Principal.

7.3 Once authorised to make online comment in a professional capacity, employees of the college are to:

- disclose they are an employee of the college and use only their own identity
- comment only on their area of expertise and authority and only on information considered to be for the public domain
- ensure that all content published is accurate and not misleading.

7.4 Employees of the college are only to contact students via their college email address or through the parent's mobile, home phone or email/home address. Any other forms of communication require the explicit approval from the relevant Head of Campus.

7.5 Social media immediately distorts relational boundaries through the use of its online language such as 'social', 'follow', 'friends', 'unfriend'.

7.6 Parents are therefore asked to respect that college employees are prohibited from becoming members of current, or newly graduated, student/s on social media. Likewise, parents should not invite a current member of staff to join their social media site/s.

7.7 Similarly, just as in their person to person interactions, each member of staff is to maintain clear online adult-child; teacher-student and professional-parent relational boundaries at all times.

7.8 Further, users who are employees of the college are required to use professional discretion before accepting past students or past parents as 'friends' on social media.

8 Monitoring by the College

8.1 For the safety and wellbeing of one another, each member of our college community is asked to adhere to the college's guidelines regarding conditions of use for student access to college hosted websites such as blogs, wikis etc. and those accessed beyond the college premises such as in the home, out of school hours on a third-party server under the supervision of the parent.

8.2 Teaching staff are to comply with college guidelines, applying the highest of professional standards, in the establishment and maintenance of online learning platforms and their site administration.

8.3 As previously stated, to maximise student safety online, the college reserves the right at any time to supervise and monitor a student's personally owned ICT, including mobile phone, on the college site or at any college related activity. The user agrees to promptly make the ICT equipment or device available to the college for purposes of any such monitoring/supervision and to otherwise co-operate with the college in the process. Before commencing the check, the college will inform the user of the purpose of the check

8.4 It is important parents are aware that devices with 4G and or 5G access built-in (including smart phones) provide the user with the capability of connecting to non-college monitored wireless networks via, for example, hot spots or cellular networks.

9 Loss or Damage

9.1 Members of our college community are responsible for the security of college owned as well as personally owned ICT equipment, including mobile phones, and devices which have been assigned to them. It is the responsibility of the user not to allow communication equipment and devices, including mobile phones, to be left unsecured, at all times.

9.2 On the Cotlew Street Campus, to minimise loss or damage, it is recommended and encouraged that student mobile phones are kept at Student Reception or handed to the class teacher for the course of the school day.

On the Ashmore Road Campus, mobile phones should not be visible unless under the direct instruction of a staff member. Devices must be kept in lockers from the time of students' arrival to school and during the course of the school day.

9.3 ICT devices and/or equipment, including mobile phones which are found on college grounds and whose owner cannot be located, are to be handed in immediately to the relevant campus Student Reception.

9.4 If, after investigation by the college, it is found that college owned ICT equipment or devices have been either intentionally damaged, or there has been an absence of due care (i.e. neglect), the user agrees to cover any incurred reparation or replacement costs. In the case of students, user refers to the student's parent/custodial guardian/carer.

9.5 Please note the security of college owned as well as personally owned ICT equipment is the student's responsibility. The college takes no responsibility for the recovery of these items if they are damaged, lost or stolen.

10 Mobile Phone/Smart Watch/ Headphones/ Earphones/ Earbuds Usage

10.1 The class teacher may allow students to use a mobile phone, smart watch and earphones/earbuds in a classroom setting under staff member's direct supervision and instruction for educational reasons.

10.2 If mobile phones/ headphones/earphones/ earbuds are brought onto the college grounds they should not be visible for lessons and college activities including chapels, assemblies and excursions,

unless under a staff member's direct supervision and instruction. Mobile phones should be placed into "silent mode."

If students need to make contact with a family member/guardian/employer he/she may do so by sending a short text message at morning tea or lunch, in a timely manner at the student's locker. If students need to make a call to someone, this must be done at Student Reception.

On the Junior Campus, all communication to parents should be done via the class teacher or reception.

Consequences for visibly using these items on college grounds include staff members confiscating the items and storing them at Student Reception until the end of the school day. Repeated instances may result in lunchtime and afterschool detentions and suspensions. Students may also be asked to sign their phones into Student Reception each day.

10.3 Students are permitted to wear smart watches, however are requested to ensure they are used in a responsible manner and are not used in any manner or place that could be deemed disruptive to the normal routine of the college. Please note the security of this item is the student's responsibility. The college takes no responsibility for the recovery of this item if it is damaged, lost or stolen.

10.4 In order to fulfil our Duty of Care to students, a member of staff must speak with a parent or custodial guardian regarding sick or injured students prior to leaving college grounds. Any student who is feeling unwell at school and needs to go home must arrange this through their relevant Student Reception. Under no circumstance may students use electronic devices such as laptops, mobile phones, iPads to contact home and make arrangements to leave the college grounds.

10.5 Parents are reminded that in cases of emergency, their relevant Student Reception remains the first point of contact ensuring your child is reached quickly and assisted appropriately.

To ensure the maximisation of class time, parents are asked not to contact their child directly using an electronic device including mobile phone or iPad during class time.

10.6 All members of our college community are reminded that it is a criminal offence to use a mobile phone to for example, menace, harass or offend another person.

11 Breach of Agreement

11.1 Breaches of this Agreement may directly or indirectly place at risk the online safety, privacy and reputation of each member of our college community and the college in general. In some situations where the breach may be deemed unlawful the college is obligated to notify the police or other relevant authority.

11.2 Compliance with the policies and procedures of the college has at all times the aim of protecting the online safety, privacy and wellbeing of each member of our college community and the college in general.

11.3 Failure to comply may result in disciplinary action, withdrawal of enrolment or termination of employment. In serious cases, such as possible breaches of child protection legislation or telecommunications legislation, the college may be obliged to notify the Police or other relevant authority.

11.4 It is important that any breach of this agreement be reported immediately. Concerns should initially be reported to your child's class teacher (Cotlew Street Campus) or either the student's pastoral care teacher or Head of Year (Ashmore Road Campus).

11.5 College employees reporting a breach are to do so in accordance with college reporting guidelines.

11.6 All reports of concern are to be treated seriously and with respect.

11.7 The privacy of the relevant parties involved will be maintained with the possible exception of where the breach may involve possible unlawful behaviour requiring a report be made to the

polices.

RELATED POLICIES AND DOCUMENTS

Acceptable User Guidelines for Students in P-3

Acceptable User Guidelines for Students in Years 4 and 5

Anti-Bullying Policy P-12

Anti-Discrimination Policy

Child Protection Policy

Privacy Policy

Relational Management Policy

Social Media Guidelines