Samaritan
COLLEGE

ICT STUDENT ACCEPTABLE USE

All digital devices (e.g. laptops, mobile phones, iPads etc.) and services – including cybersafety expectations.

To be read in conjunction with Catholic Education SA's (CESA) policies on ICT found on the college website.

PREAMBLE

The use of digital devices and points of access to e-mail and Internet services at Samaritan College is provided to students in order to support their educational and administrative needs. These digital devices and services are educational tools and **must be used in a responsible manner**. This policy recognises that there are constant advances and changes in the use of technology (including for e.g. software, apps, information sharing, social media platforms, new devices etc and this list is not exhaustive). Therefore students must seek advice and clarification from the school as soon as possible when engaging with new or unfamiliar technology. Acceptable use is guided by the following principles.

- Students must behave in an ethical manner when using ANY digital device to access resources, communicate and interact with others.
- Online behaviour should at all times demonstrate respect for the dignity of each person.
- It is **never acceptable** to use digital devices to harass, bully or humiliate others.

This document informs parents and students of our school's expectations when students are using the devices and services provided whether provided by the school or BYOD, and when using their personal equipment to communicate to or about members of the wider school community.

Students whose actions contradict this policy may be subject to further action and consequences. This may include the withdrawal of access to services, referral to SAPOL, internal consequences or suspension/expulsion.

Unacceptable material may be supplied to the SA Police or other relevant agency (for e.g. Family & Community Services etc) at the discretion of school or CESA personnel.

The school reserves the right to capture, store and review all online activity and content created or accessed via school provided services. Such material is the property of the school and CESA. A student-owned device may be taken (and then accessed with a parent or SAPOL present) where there is a reasonable belief that:

- There has been or may be a breach of the school rules or policy
- There may be a threat of harm to a student or others or system security.

STUDENTS USING SCHOOL OWNED TECHNOLOGY

Students who use a school owned device have the following responsibilities:

- To care for the laptop / device to the best of their ability.
- To keep the laptop / device secure and protect it from any malicious damage.
- To replace or repair any damaged, lost or stolen laptop / device at their own cost.

APPROPRIATE USE

1. *When using school and/or personal devices and services* ***students will****:*

- ensure that they access the Internet only within the school proxy and filtering system provided.
- ensure that communication through Internet and email services is related to learning.
- keep passwords confidential, current and private.
- log off at the end of each session to ensure that nobody else can use their account.
- promptly tell their teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- seek advice if asked, online, for personal information i.e. address, credit card, to meet etc
- Use appropriate privacy controls for all internet and app based activities. i.e. location settings
- ensure that school services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.
- conduct consistent with the Catholic ethos of the college
- behave ethically and responsibly in all dealings with others.
- observe obligations regarding confidentiality and privacy.
- select and maintain (i.e. change regularly) a secure password and ensure you do not provide the password to anyone else.
- do not attempt to gain unauthorised access to anyone else’s account or user information, or otherwise attempt to defeat any security controls.
- restrict use of devices that record others or take photos.
- report any suspicions of unauthorised or inappropriate access to the school.
- treat equipment with care.
- take home any devices/equipment supplied to them by the school.
- report to an adult if cyberbullied or if they see/hear anything online that makes them feel uncomfortable
- When using Artificial Intelligence or ChatGPT type software, adhere to the current SACE (Year 10-12) Policy or relevant copyright/plagiarism processes when using AI in school work i.e. acknowledging sources. Students will understand that the teacher may ask for proof of his/her work in some circumstances. Use of AI is not an excuse for work containing inappropriate images or comments i.e. blame ChatGPT.

2. *When using the school services or personal mobile phones (or similar personal equipment)* ***students will not, and will not attempt to:***

- disable settings for virus protection, spam and internet filtering that have been applied by the school and not attempt to evade them through use of proxy sites.
- disable systems such as, but not limited to, desktop images or screensavers
- allow others to use their personal accounts.
- deliberately use the digital identity of another person to send messages to others or for any other purposes.
- enter ‘social networking’ sites/apps

- intentionally download unauthorised software, graphics or music that are not associated with the learning activity as directed by a staff member.
- damage or disable computers, computer systems or networks or distribute damaging files or viruses.
- disclose personal information about another person (including name, address, photos, phone numbers)
- distribute or use information which is copyrighted without proper permission.
- take photos or video of members of the school community without their consent.
- send or publish any statement, image or other material that is offensive or threatening, or could constitute harassment, discrimination, vilification, defamation or bullying. This can simply include sending or publishing any image without the permission of those in the image. And includes the use of swear words or any other offensive language – especially in email.
- knowingly access, download, store, send or publish any material that is pornographic.
- do anything that you know, or reasonably suspect could contravene the law, including without limitation downloading material in breach of copyright.
- send or help to send unsolicited bulk email (spam).
- open or download any attachment, or access any link, that you reasonably suspect may contain a virus, malware or other computer contaminant.
- install unlicensed or non-approved software onto any supplied computers or communication devices.
- use ICT Facilities to cheat or plagiarise.
- use ICT Facilities to store or download files for personal use.

3. *We repeat……when using ICT to communicate or publish digital content students must* ***never*** *include:*

- unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
- threatening, bullying or harassing material or make unreasonable demands.
- sexually explicit or sexually suggestive material or correspondence.
- false or defamatory information about a person or organisation.
- the school name or crest without the written permission of the Principal/Deputy or Campus Head.

This Procedure document also addresses the particular use of these technologies that has come to be referred to as **'Cyberbullying'.** The school will investigate and take action where this kind of bullying occurs in school **and** outside of school when it causes significant harm to the relationships between students and or teachers or is criminal in nature or has the capacity to impact on relationships across the wider school community.