Policy number	006		
Drafted by	Mary-Anne Revell	Last Approved by Executive	September 2021
Responsible person	Steven Nicholas	Scheduled review date	September 2024

Definitions of terms used in these guidelines.

a. **'Authorised user'** means a person who has signed the eSmart Agreement (or has had it signed on their behalf by a parent) and is authorised by the College to use College ICT.
b. **'eSmart'** refers to the name of the cybersafety guidelines that are followed at Olivet Christian College to promote the safe, responsible and ethical use of ICT.
c. **'ICT'** stands for 'Information and Communication Technologies' and includes network facilities, communication technologies, eLearning tools and ICT equipment/devices.
d. **'Network facilities'** includes, but is not limited to, the internet access to files, web sites and digital resources via the College network.
e. **'Communication technologies'** includes, but is not limited to, communication made using ICT equipment/devices such as internet, email, instant messaging, online discussions/surveys and mobile phone activities and related applications.
f. **'eLearning'** refers to the use of ICT for educational purposes.
g. **'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.
h. **'Agreement'** refers to the eSmart Agreement which will be reviewed annually.
i. **'College'** means Olivet Christian College.
j. **'College related activity'** includes, but is not limited to, an excursion, camp, sporting or cultural event, wherever its location.
k. **'College ICT'** refers to any ICT owned or operated by the College including, but not limited to, network infrastructure, computers, cameras, tablet devices.
l. **'Objectionable material'** includes, but is not limited to, pornography, cruelty, violence, or material of a discriminatory nature that it is likely to be detrimental to the wellbeing of students or unsuitable to a College environment.
m. **'Unacceptable student 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 or copyright infringement.
n. **'Educational purposes'** means activities that are directly linked to curriculum related learning.
o. **'Personal electronic devices'** includes, but is not limited to, handheld gaming consoles (incuding but not limited to Nintendo DS, PSP Wii U), MP3 players (including but not limited to iPod, iPod Touch), e-readers (including but not limited to Kindle, Kobo) other internet and 3G accessible devices, and any other similar such devices as they come into use.

Purpose

Our aim is to provide an educative environment by establishing an eSmart culture which is in keeping with the values of the College, legislative and professional obligations, and the community's expectation. Within this context, the objectives of these guidelines are to ensure the smart, safe, responsible use of ICT within the College community.

These guidelines outline the conditions applying to the use of all College ICT and behaviours associated with safe, responsible and ethical use of technology. Authorised users are required to comply with the Agreement.

1. Authorised Usage and eSmart Agreement

1.1. As the College provides network access, the contents of the College ICT system, including email messages, remain the property of the College. The College has the capacity to monitor and control the system and reserves the right to monitor individual usage and report, where necessary, any indications of misconduct or prohibited use.

1.2. All users, whether or not they make use of network facilities and communication technologies on College owned or personal ICT equipment/devices, will be issued with this Agreement. This document should be read carefully with the acknowledgement page signed and returned to the student's class teacher.

1.3. The College's ICT, including network facilities, communication technologies, and ICT equipment/devices cannot be used until the acknowledgement page of this Agreement has been signed and returned to the student's class teacher. Signed Agreements will be filed in a secure place.

2. Obligations and requirements regarding appropriate use of ICT in the College learning environment

1.1. While at College, using College owned or personal ICT equipment/devices is for educational purposes only.

1.2. When using College or privately owned ICT on the College site or at any College related activity prohibited use includes, but is not limited to, any conduct that is defined as objectionable and inappropriate:

- Would cause offense to students, teachers or parents, such as profanity, offensive language, obscenity, pornography, unethical or illegal solicitation, racism, sexism,
- is derogatory or threatening to another e.g. Libelous, slanderous, inflammatory, threatening, harassing;
- has intention to deceive, impersonate or misrepresent;
- Forwards confidential messages to persons to whom transmission was never authorised by the College, including persons within the College community and persons/organisations outside the College community
- Fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus
- Breaches copyright
- Attempts to breach security and infrastructure that is in place to protect user safety and privacy
- Results in unauthorised external administration access to the College's electronic communication
- Propagates chain emails or uses groups or lists inappropriately to disseminate information
- Inhibits the user's ability to perform their duties productively and without unnecessary interruption,
- Interferes with the ability of others to conduct the business of the College
- Involves malicious activity resulting in deliberate damage to College ICT and/or ICT equipment/devices.
- Involves the unauthorised installation and/or downloading of non-College endorsed software
- Breaches the ethos and values of the College Is illegal

2.3. In the event of accidental access of such material, Authorised Users must:

- Not show others
- Shut down, close or minimise the window
- Report the incident immediately to the supervising teacher.

2.4. A person who encourages, participates or otherwise knowingly acquiesces in prohibited use of College, or privately owned communication technologies, on the College site or at any College related activity, may also be found to have engaged in prohibited use.

2.5. While at the College or a College related activity, Authorised Users must not have involvement with any material which might place them at risk. This includes images or material stored on privately owned ICT equipment/devices brought onto the College site, or to any College related activity such as USB sticks.

2.6. Authorised users must not attempt to download, install or connect any unauthorised software or hardware onto College ICT equipment, or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, and any other similar technologies that are available. Any Authorised Users with a query or a concern about that issue must speak with the relevant class teacher or subject teacher.

3. Monitoring by the College

The College:

3.1. Reserves the right at any time to check work or data on the College's computer network, email, internet, computers and other College ICT equipment/devices, without obtaining prior consent from the Relevant Authorised User.

3.2. Reserves the right at any time to check work or data on privately owned ICT equipment on the College site or at any College related activity. The Authorised User agrees to promptly make the ICT equipment/device available to the College for purposes of any such check and to otherwise co-operate with the College in the process. Before commencing the check, the College will inform the Authorised User of the purpose of the check.

3.3. Monitors traffic and material sent and received using the College's ICT infrastructures. From time to time this may be analysed and monitored to help maintain an eSmart learning environment.

3.4. From time to time conduct an internal audit of its computer network, internet access facilities, computers and other College ICT equipment/devices, or may commission an independent audit of content and usage.

4. Copyright, Licensing, and Publication

1.1. Copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Authorised Users must not breach laws of copyright, moral right or intellectual property – this includes illegal copies of software, music, videos images.

1.2. All material submitted for internal publication must be appropriate to the College environment and copyright laws.

4.3. Any student/s found to use an ICT equipment/device to gain advantage in exams or assessments will face disciplinary actions as sanctioned by the College.

5. Individual password logons to user accounts

5.1. If access is required to the College computer network, computers and internet access using College facilities, it is necessary to obtain a user account from the College.

5.2. Authorised Users must keep usernames and passwords confidential and not share them with anyone else. A breach of this rule could lead to users being denied access to the system.

5.3. Authorised Users must not allow another person access to any equipment/device logged in under their own user account. Material accessed on a user account is the responsibility of that user. Any inappropriate or illegal use of the computer facilities and other College ICT equipment/devices can be traced by means of this login information.

5.4. Those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with the Guidelines and Agreement. This includes ensuring that no electronic communications could cause offence to others or harass or harm them, put the owner of the user account at potential risk, contain objectionable material or in any other way be inappropriate in the College environment.

5.5. For personal safety and having regard to Privacy laws, Authorised Users must not reveal personal information about themselves or others online. Personal information may include, but is not limited to, home addresses and telephone numbers.

6. Other Authorised User obligations

6.1. Avoid deliberate wastage of ICT related resources including bandwidth, through actions such as unnecessary printing and unnecessary internet access, uploads or downloads.

6.2. Avoid involvement in any incident in which ICT is used to send or display electronic communication, graphics, audio, video files which might cause offence to others and/or involve objectionable material.

6.3. Abide by copyright laws and obtain permission from any individual before photographing, videoing or recording them.

7. Privacy

7.1. College ICT and electronic communication should never be used to disclose personal information of another except in accordance with the College's privacy agreement or with proper authorisation. 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. Authorised users must take responsibility for the security of their computer and not allow it to be used by unauthorised persons.

7.2. While after College use of communication technologies 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. Any such behaviour that impacts negatively on the public standing of the College may result in disciplinary action.

The College takes a strong position to protect privacy and prevent personal information and opinion being published over technology networks including Facebook, YouTube, Tumblr (and any further new technology).

8. Procedures for Mobile Phone and Other Electronic Device Use at College

Olivet Christian College accepts that some parents provide their children with mobile phones and other personal electronic devices. However, whilst on College property and during College excursions and camps, use of mobile phones or personal electronic devices is not permitted by students unless specifically authorized by the Principal.

Responsibility

8.1 It is the preference of the College that mobile phones and personal electronic devices are not to be brought to college. Th e College takes no responsibility for replacing lost, damaged, or stolen phones either at the College or travelling to and from school.
8.2 It is the responsibility of students who do bring mobile phones or personal electronic devices onto college premises to adhere to the guidelines outlined in this document.
8.3 Mobile phones should be left in students' bags and turned off (or on silent) for the duration of the school day, or whilst they on excursions, camps and extra-curricular activities.
8.4 If the phone is discovered in the student's possession it will be confiscated and handed into the office. It will be returned at the Principals discretion.
8.5 If a phone is taken into the toilet blocks it will be confiscated and returned at the Principals discretion.'
8.6 In case of emergency parents/guardians or employers can contact the school
8.7 Phones taken on excursions, camps or extra-curricular activities must be handed in to the teacher until required. In some instances, the phones may be left at school.

Teachers should use this document to discuss and teach the safe and responsible online behaviours that the College expects of its students. This should be sent home for parents to further discuss with their children and to promote and reinforce safe and responsible online behaviour at home.

When I use digital technologies I:

Communicate respectfully by thinking and checking that what I write or post is polite and respectful.
This means:
- never sending mean or bullying messages or passing them on, as this makes me part of the bullying
- not using actions online to be mean to others. (This can include leaving someone out to make them feel bad)

- not copying someone work or ideas from the internet and presenting them as my own (I will include the link).

Protect personal information by being aware that my full name, photo, birthday, address and phone number is not to be shared online.

This means:

- protecting my friends' information in the same way
- protecting my password and not sharing it with others
- only joining a space online with my parents or teacher's guidance and permission
- never answering questions online that ask for my personal information.

Look after myself and others by thinking about what I share online.

This means:

- never sharing my friends' full names, birthdays, College names, addresses and phone numbers because it is their personal information
- speaking to a trusted adult if I see something that makes me feel upset or if I need help
- speaking to a trusted adult if someone is unkind to me
- speaking to a trusted adult if I know someone else is upset or scared
- stopping to think about what I post or share online
- using spaces or sites that right for my age
- not deliberately searching for something rude or violent
- either turn off the screen or use the back button if I see something I don't like and telling a trusted adult
- being careful with the equipment I use.

Conditions:

When I use digital technologies I:

- **communicate politely and respectfully**

This means that I will:

- write nice things to other people
- not make someone feel sad
- never sending mean or bullying messages or passing them on, as this makes me part of the bullying
- not using actions online to be mean to others. (This can include leaving someone out to make them feel bad)
- not copying someone work or ideas from the internet and presenting them as my own (I will include the link).

- **protect personal information**

This means that I will

- not share my photo online

- **look after myself and others** by thinking about what I share online

This means that I will

- not share my friends photo online
- tell my teacher or a trusted adult if someone is unkind to me
- never sharing my friends' full names, birthdays, College names, addresses and phone numbers because it is their personal information
- speak to a trusted adult if I see something that makes me feel upset or if I need help
- speak to a trusted adult if someone is unkind to me
- speak to a trusted adult if I know someone else is upset or scared
- stop to think about what I post or share online
- use spaces or sites that right for my age
- not deliberately searching for something rude or violent
- either turn off the screen or use the back button if I see something I don't like and telling a trusted adult
- be careful with the equipment I use

Evaluation: This policy will be reviewed as part of the three-year review cycle