Rationale

At Hope Christian College (HCC), we understand that Information and Computing Technology (ICT) is part of everyday life. The use of ICTs at the College is governed by our Christian principles and understandings. The College's ICTs are used in all forms of learning and the advancement of knowledge and personal understanding. The same standards of communication and interaction apply to ICTs as they do to face-to-face communications.

Aim

This policy seeks to set down an overarching procedure and clear expectations guiding the College community on how ICTs should be used in the College environment. Students should also refer to the most current edition of the *Student Portable Device Program Handbook* and refer to it in conjunction with this policy.

Policy Statement

Student's use of ICTs at HCC must be strictly in line with the conditions outlined in this policy. Students and parents/caregivers are required to sign all applicable agreements prior to commencing use of ICTs at HCC. College ICTs are to be used safely and for educational use only.

Scope

This policy outlines the acceptable use of ICTs for HCC students whilst engaging in their learning both on and off campus and outlines acceptable standards of behaviour with College ICTs.

Definitions

at/to the College – this refers to being on the College grounds, but also refers to being present at College activities such as excursions, on or off site, and special days (e.g. Sports Days) and requires adherance to this policy unless specified by a separate policy or when specific permission is given by the responsible staff member

College community – this includes but may not be limited to: students, parents of students, immediate family of students (particularly minors like younger siblings), authorised volunteers, authorised visiting speakers and guests, staff (whether temporary, contracted or permanent), staff spouses and dependant children (who are not staff or family), College leadership, and CCC church staff and leadership that are connected in some way to the College (e.g. not unconnected church attendees).

departmental head – refers to the Principal, an appropriate deputy or coordinator

'friend'– in a social media sense, to allow or accept access to another's social media account; this includes 'friending" on sites like *Facebook* or *Snapchat* and 'following' on site such as *Instagram* or *Twitter*

ICT - Information and Computing Technology in any form

mobile phone – also refers to any devices such as *Apple watches* or similar devices or applications that are able to function in the capacity of a phone

parent – includes caregivers and guardians, or the responsible person as listed on the enrolment form

social media – refers to online communities sharing comments and content, via web or apps

staff, staff members– refers to the student's class teacher or a paid Hope Christian College staff member who is responsible for supervising the student during College hours or activities

student – any student enrolled at Hope Christian College through a contract with their parent/guardian(s), regardless of their age

Overarching conditions for all College ICT use

- Students may not use a non-College issued device whilst on campus. HCC has adopted a 'Standard Operating Environment' ensuring that all students have equitable access to appropriate ICTs and IT support in the event of a fault or problem.

- There is 'no expectation of privacy' when using College issued ICTs. This includes hardware, storage (local, network, or cloud), and any data received or transmitted using College-owned accounts (e.g Google Drive, email, etc).

- The College retains control, custody, and supervision of all computers, networks, and Internet services owned or leased by the College.

- All students who are a part of the portable device program are required to bring their laptops to school fully charged, beginning the day with a battery level between 80% and 100%. This enables uninterrupted engagement in educational activities and prevents any hindrances caused by insufficient battery life, while also reducing the risk of accidents that may arise from charging cables and power outlets.

- The College reserves the right to monitor all computer and Internet activity by students using College equipment, networks or accounts.

- Student and/or student's parents/caregivers shall be responsible for compensating the College for any costs due to loss or damage (deliberate or accidental) arising from the misuse of ICTs and their consumables (e.g. power packs, cords, carry bags).

- No member of the College community may use any College ICT for illicit or illegal activities and may not use methods such as proxy servers to bypass College network security, whether on site or elsewhere. Illegal use will be referred to the Police.
- In the event of loss or theft of College ICTs, a Police Report and Incident Number must be obtained, and the loss reported to the student's Home Group Teacher, and IT Manager as soon as possible.

Restrictions of hardware and software use

If a fault is encountered, students must report this to the closest responsible staff member who may direct the student to the IT Office, and ensure that the device is adequately protected during transit, i.e. College Laptop should be transported in College-issued Laptop bag...

Students are not permitted to do any of the following with College ICTs:

- install, copy, or delete software unless installing available software through the College Software Centre App
- remotely control or message any other computer
- change computer system settings or attempt to bypass network security protocols or settings in any way whatsoever (e.g. proxy servers)
- play games unless under the direction and supervision of a staff member
- download or stream audio or video content without the staff member's permission
- use an external wireless network while at College (e.g. tethering to mobile devices) using a personal laptop, mobile phone or any other portable networking device.
- use student email accounts for anything other than academic purposes.

Students may have their internet access revoked (Blacklisted) if they are found to be using the internet for non-school related purposes.

Data storage and retrieval

Instructions on the storage of College related data will be given at the beginning of the school year, however it remains the responsibility of the student to save and back up their work. Loss of data will not be accepted as an excuse for late, or non-submission of work. All College related data should be saved and backed up on the College network (Years 1-5) and Google Drive File Stream (Years 6 – 12).

Students must:

- immediately report any interference to their personal files or email

- not store personal files on any College device or College-issued cloud storage without permission from a staff member

- not attempt to access files that belong to another student or staff member

- never use their own ICT devices (phones, mp3 players, etc.) or for data storage at College.

Security and cyber-safety

Students will be educated as part of their educational program about online security and cyber-safety. Passwords will expire and need to be updated on a regular basis. Students should never log on to the network with anyone else's username and password, or device, nor let anyone else know their password. Students must immediately report any suspicious activity to a teacher regardless of how harmless it may seem.

A student must not, without permission from a staff member:

- reveal their personal information on the Internet
- go to any site not specifically College work related
- go to chat rooms or use any social networking sites or personal blogs (e.g. Facebook, Twitter) at College.

Additionally, a student must never:

- click on any advertising material
- view or transmit any content that is offensive, or compromises the Christian values of HCC including, but not limited to, pornography and other sexually explicit content, violent and/or hatred-inciting content, criminal activity, child abuse, self-harm, and other malicious content.
- distribute or publish any media stored on the College's server (e.g. copying a photo from the media drive and posting on Facebook). All media remains the property of the College.

Conditions for student portable device (laptop) use

Please see the must current edition of the *Student Portable Device Program Handbook* (revised yearly) for more detailed information concerning correct use of College-issued laptops.

Prohibitions whilst using College ICTs

Students must observe and follow the following:

- food and drink must not be consumed whilst using College ICTs and related equipment.
- devices must not be used during recess and lunch without the permission of a staff member
- do not attempt to fix any college equipment (including their own device) themselves but report the broken item to the IT Department immediately.

Any breach of these conditions will result in College discipline. See *Behavioural Management Policy.*

Other relevant policies and publications:

- HCC Privacy Policy
- HCC Mobile Phone Use Policy
- HCC Social Media Use Policies
- HCC Recording & Image Use Policy
- HCC Behavioural Management Policy
- Staff Conduct Policy
- Staff Handbook
- Student Portable Device Program Handbook (current edition)

Review

The policy will be reviewed every two years. Reviews will be conducted by the responsible officer, drawing upon input and feedback from staff and leadership of the College, and the *Association of Independent Schools of South Australia (AISSA)* who will advise on external changes, such as changes to legislation, good practice, etc.