COMPUTER & INTERNET ACCEPTABLE USE POLICY

Postal Address: PO Box 252 Cloverdale Western Australia 6985
Tel: (618) 9362 5340 Email: info@aic.wa.edu.au **Website:** www.aic.wa.edu.au

Thornlie College: 17 Tonbridge Way, Thornlie Tel: 9493-2718
Dianella College: 81 Cleveland St, Dianella Tel: 9375-9770
Kewdale College: 139 President St, Kewdale Tel: 9362-2100

COMPUTER & INTERNET ACCEPTABLE USE POLICY

1. PURPOSE

The purpose of this policy is to set out policies and guidelines for access to, and use of, the College's computer system and acceptable use of the Internet and to regulate their acceptable use.

2. GENERAL STATEMENT OF POLICY

Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the college computers and to the Internet enables students to explore thousands of libraries, databases, and other resources while communicating with people around the world. The College expects that the staff will integrate thoughtful use of the computers and the Internet throughout the curriculum and will provide guidance and instruction to students in their use. While recognising that the Internet is largely unregulated and contains a great deal of harmful material, restricting its use to lawful educational uses is the best protection for all against unexpected and unwanted material.

3. EDUCATIONAL PURPOSE

The College is providing students with access to the computers, which includes Internet access. The purpose of the computers is not to provide students with general access to the Internet. The computers are used for educational purposes only, which includes use of the computers for classroom activities and assignment research. Users are expected to use Internet access through the network to further educational and personal goals consistent with the mission of the College and school policies. The computers and network are not intended for student or staff personal use, and uses which might be acceptable on a user's home computer may not be acceptable on the college's network.

4. USE OF COLLEGE COMPUTERS IS A PRIVILEGE

The use of the computers and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the College's computers or the Internet may result in one or more of the following consequences: suspension or cancellation of use of access privileges; payments for damages and repairs; discipline under other appropriate College policies, including suspension or exclusion; or civil or criminal liability under other applicable laws.

5. UNACCEPTABLE USES

The following uses of the College's computers and Internet resources or accounts are considered unacceptable.

Users will not use the computers to:

a. Access, review, upload, download, store, print, post, email or distribute pornographic, obscene, sexually explicit or lewd material.

b. Transmit or receive obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, harassing, or sexually explicit language.

c. Access, review, upload, download, store, print, post, e-mail, or distribute un-islamic content and content not in line with the college values and ethos.

d. Access, review, upload, download, store, print, post, or distribute materials that use language or images that are inappropriate to the educational setting or unrelated to an educational purpose.

e. Access, review, upload, download, store, print, post, e-mail, or distribute materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment or discrimination.

f. Knowingly or recklessly post false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

g. Use any computer or network resource for personal use, including to play games, to download or transfer material for personal use, or to access or view material not directly related to educational purposes.

h. Vandalise, damage or disable the property of the College, another person or organisation, or to make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means.

i. Tamper with, modify or change the College computer software, software configurations, control panel settings, hardware or cabling.

j. Take any action to violate or attempt to violate the College’s system's security.

k. Use the College system in such a way as to disrupt the computer usage by other users.

l. Gain unauthorized access to information resources or to access another person's materials, information or files without the direct permission of that person.

m. Post private information or data about another person or to post personal contact information about themselves or other persons including, but not limited to, photos, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, and will not re-post a message that was sent to the user privately without permission of the person who sent the message.

n. Attempt to gain unauthorized access to the College's network or any other computer of the College's network, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user even if the unauthorised access password had been freely given to the unauthorised user.

o. Violate copyright laws, or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software, or copying software to or from any school computer, and the plagiarizing of works found on the Internet

If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to the Head of Information Technology or the Principal. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. It is understood that all sites visited by a user is recorded and stored on the College servers. Evidence of inappropriate use will be pursued and claims of unauthorised use of an account will not be an acceptable defence. It is the students' responsibility to protect the integrity of their access passwords and they should not pass them on to any other person for any reason whatsoever.

Staff members are not to give access to their work computer or any other work device to their children or family member. This includes at work and after work.

6. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the College computer system and use of the Internet shall be consistent with College policies and the mission of the College.

7. LIMITED EXPECTATION OF PRIVACY

a. By authorizing use of the computers, the College does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on the College system.

b. Routine maintenance and monitoring of the College computers involving checks on browser history may lead to a discovery that a user has violated this policy, another College policy, or the law.

c. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or College policy.

d. The College has the right at any time to investigate or review the contents of students' files and e-mail files. Parents have the right to request of the College, an examination of their child's individual account at any time if they suspect inappropriate use.

e. The College will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities and activities not in compliance with College policies conducted using College's computers.

8. INTERNET USE AGREEMENT

a. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents and staff of the College.
b. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet.

c. The Internet Use Agreement form must be read and signed by the user and the parent or guardian. The form will then be filed at the College office.

9. LIMITATION ON COLLEGE'S LIABILITY

Use of the College system is at the user's own risk. The system is provided on an "as is, as available" basis. The College will not be responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data stored on College's diskettes, tapes, hard drives or servers, or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause.

The College is not responsible for the accuracy or quality of any advice or information obtained through or stored on the College computers. The College will not be responsible for financial obligations arising through unauthorised use of the College's computers or the Internet.

10. CYBER SECURITY

Cyber attacks occur when there is an attempt or actual incident by hackers to damage or destroy a computer network or system. It is not uncommon for a student to hack their own school. Therefore the College makes its stance clear on the acceptable use of and access to its IT and online environments. It is essential for students and parents to know, understand and accept that there are serious penalties for students who attempt to hack into or manipulate the school's IT systems. It is also important to know that these penalties involve more than just school sanctions. In order to prevent an attack, school staff and management should take the necessary steps:

<u>Staff</u>

- Use complex passwords, changing them often, not sharing them or writing them down.
- Not leave personal computers unattended: if a staff member leaves a personal computer unattended for an extended period of time, they should log out or lock the screen. Staff should set computers to automatically lock the screen after a period of inactivity;
- When a teacher leaves a classroom for a break or to attend another lesson, the teacher should take the laptop, tablet or other device with them; and

- Staff must not share or give access to their laptop, tablet, computer or other device to students for any matter at any time.

School

- Have the IT staff conduct regular tests to protect school computer systems against cyber attacks or hacks. These tests are vital to assess a school computer system's ability to prepare, respond, recover and prevent an attack. A cyber attack or hack not only can retrieve information from a system but it can also immobilise it; rendering it useless.
- To help guard against a cyber attack, schools can install anti-virus software, restrict access of administrator privileges to certain key staff and change staff passwords on a regular basis.
- Educating staff and students on cyber security will assist to reduce the risk of a cyber attack. If employees or contractors are aware of how cyber attacks can occur, this may prevent possible attacks on school computer systems.
- Education on cyber awareness can be achieved through professional development workshops, seminars or other courses related to cyber security.

Both staff and the school have a responsibility to ensure the possibility of a cyber attack does not arise.

Implementation date: [February 2018]

Approved by: [Executive Principal]

Next review: [February 2019]

INTERNET USE AGREEMENT

STUDENT

I have read and understood the College's policies relating to acceptable use of the College's computer system and the Internet and agree to abide by them. I further understand that any violation of the policies above is unethical and may constitute a violation of law. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken.

User's Full Name (please print): _____

User Signature: _____ Date: _____

PARENT OR GUARDIAN

As the parent or guardian of this student, I have read the College's policies relating to acceptable use of the College's computer system and the Internet. I understand that this access is designed for educational purposes. However, I also recognise it is impossible for the College to restrict access to all controversial materials and I will not hold the College or its employees or agents responsible for materials acquired on the Internet. I hereby give permission to issue an account for my child.

Parent or Guardian's Name (please print):

_____

Parent or Guardian's Signature: _____