Internet Access Policy

Postal Address: PO Box 252, Cloverdale, WA 6985
Ph: (618) 9362 5340 Email: info@aic.wa.edu.au **Website:** www.aic.wa.edu.au
Thornlie College: 17 Tonbridge Way, Thornlie Ph 9493 2718
Dianella College: 81 Cleveland Street, Dianella Ph 9375 9770
Kewdale College: 139 President Street, Kewdale Ph 9362 2100

Table of Contents

Internet Access Policy

1. Purpose

The College is committed to providing a safe and secure online environment for staff and students through the implementation of security and compliance standards. It is the responsibility of every student and employee of the College to ensure that Information, Communication and Technology (ICT) resources are never used to abuse, vilify, defame, harass, degrade or discriminate against others in line with the College's Anti-Bullying Policies.

2. Scope & Responsibility

This Internet Access Policy applies to all College staff who have access to computers and the internet for the performance of their work. Use of the internet by College staff is permitted and encouraged where such use supports the goals and objectives of the business. Although access to the internet through the College's computer network is a necessity for most staff to perform their duties and all staff must adhere to the College's policies concerning computer, email and internet access and usage.

The College's student learning and collaboration environment encourages the use of technology through online resources and internet connected devices. The responsible use of these devices and resources, with the guidance of the College teaching staff, will ensure a safe and secure online experience.

3. Policy Details

The Internet provides access to vast amounts of data, pertaining to almost any topic. The ICT infrastructure has been designed and is being maintained to reduce any unforeseen risks that may be encountered from time to time, however, the safe operation of devices within the school will be managed by the teachers during class. This policy is designed to provide clear guidelines about these responsibilities and must be adhered to by all staff and students.

3.1 Internet & Email Access

- 3.1.1 The internet connection is provided to Staff and Students for the intention of learning and research. Deliberate attempts to seek or use material that is illegal, or which would be regarded by reasonable persons as offensive, is not permitted.
- 3.1.2 Internet and email access are considered a privilege and not a right; as access involves responsibility. The depth of this responsibility and conveying the standards is a joint responsibility between the staff, student, families and the College.
- 3.1.3 College hardware is protected by password and is kept secure by lock and key, and at no point should a 3rd party be allowed access to these devices in an unsupervised manner.

3.2 Staff Access

- 3.2.1 Access is granted to the internet in support of lesson preparation, record keeping, resource printing, communication regarding school activities and other activities to support the learning of the children at the school.
- 3.2.2 Only software and programs installed by the ICT Department will be allowed for use by the students. It is considered illegal to copy copyrighted applications contrary to the College's License Agreement.
- 3.2.3 Disabling, uninstalling or exiting College installed applications is not permitted.
- 3.2.4 Staff must not seek out inappropriate material or applications; including but not limited to; pornographic material, material with obscene language or any explicit or sexually suggestive material.

3.2.5 Staff devices (laptops or desktops) are considered the property of the College and are enabled to connect to the secure staff network within the school. Access to these devices should not be issued to students for any reason without prior written consent from the Principal or ICT Manager.

3.2.6 Staff are responsible for protecting their own passwords.

3.2.7 Staff are responsible for protecting the confidentiality of documents available through their devices and must not leave confidential materials on the screen while they are away from their desk.

3.3 Student Access

3.3.1 Access is granted to the internet for students to research and learning.

3.3.2 Only software and programs installed by the ICT Department will be allowed for use by the students. It is considered illegal to copy copyrighted applications contrary to the College's License Agreement.

3.3.3 Disabling, uninstalling or exiting College installed applications is not permitted.

3.3.4 Abuse or deliberate misuse of the Internet connected device or online resources may result in disciplinary action, which could include bans from accessing the internet or using the College devices.

3.3.5 If students are found misusing their access to the internet or email by sending abusive letters / emails or accessing offensive material the matter will be referred to the Principal for appropriate disciplinary action in line with the Behaviour Management Policy.

3.3.6 Students are to respect the privacy and ownership of others' work at all times. This includes not plagiarising downloaded information and presenting it as their own work or copying work of other students.

3.3.7 Students must not seek out inappropriate material or applications; including but not limited to pornographic material, material with obscene language or any explicit or sexually suggestive material.

3.3.8 Students are responsible for protecting their own passwords by logging off at the end of every class, not sharing their passwords with their peers and not mismanaging their passwords (resulting in continual password resets during class).

3.4 Responsibilities

3.4.1 All inappropriate use of the internet will be reported to the Principal, ICT Manager and/or Head of the Department including the name of the person or persons involved, the location where known and the time of the incident.

3.4.2 Any external disk must be scanned for viruses prior to being used on any College computer.

3.4.3 In the event that a Virus is detected on a College owned device, the issue must immediately be reported to the ICT Department onsite with details relating to how the issue was identified to ensure the security of the network has not suffered and that the virus can be contained and removed accordingly.

4. Breaches

- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- A student found to have violated this policy will have the Behaviour Management and Student Wellbeing Policies enacted.
- The Principal has the final say in deciding what is or is not regarded as offensive in the context of the College.

5. Relevant Internal References

- ICT Acceptable Use Policy
- Network Security Policy

Review Date: [February 2020]
Approved by: [Executive Principal]
Next review: [February 2021]