



AUSTRALIAN
ISLAMIC COLLEGE

COMPUTER & INTERNET ACCEPTABLE USE POLICY

Postal Address PO Box 252, Cloverdale, WA 6985
Ph 08 9362 2100 **Email** info@aic.wa.edu.au **Website** www.aic.wa.edu.au

Thornlie College 17 Tonbridge Way, Thornlie, WA 6107 **Ph** 08 9493 2718
Dianella College 81 Cleveland Street, Dianella, WA 6108 **Ph** 08 9375 9770
Kewdale College 139 President Street, Kewdale, WA 6105 **Ph** 08 9362 2100
Forrestdale College 651 Nicholson Road, Forrestdale, WA 6112 **Ph** 08 9493 5819
Henley Brook College 10 Asturian Drive, Henley Brook, WA 6055 **Ph** 08 9375 9892
Adelaide College 22A Cedar Avenue, West Croydon, WA 5008 **Ph** 08 8340 7799

Table of Contents

1. PURPOSE	3
2. POLICY STATEMENT	3
3. SCOPE AND RESPONSIBILITY	3
4. EDUCATIONAL PURPOSE.....	3
5. USE OF COLLEGE COMPUTERS IS A PRIVILEGE	3
6. UNACCEPTABLE USES.....	3
7. CONSISTENCY WITH OTHER SCHOOL POLICIES	3
8. LIMITED EXPECTATION OF PRIVACY	4
9. INTERNET USE AGREEMENT	4
10. LIMITATION ON COLLEGE’S LIABILITY	4
11. CYBER SECURITY.....	4
APPENDIX 1: INTERNET USE AGREEMENT	5

1. PURPOSE

The purpose of this policy is to define and regulate the appropriate use of the College's computer systems and the Internet to ensure safe, responsible, and educational access.

2. POLICY STATEMENT

Access to the College's computer network and Internet resources is fundamental to developing the skills students need for educational and professional success. The College expects that staff and students will use computers and the Internet responsibly and in ways that align with the mission and values of the College. Given the unregulated nature of the Internet, restrictions are necessary to maintain an educational environment free from inappropriate and harmful content.

3. SCOPE AND RESPONSIBILITY

This policy relates to all staff including volunteers and students.

4. EDUCATIONAL PURPOSE

The College provides access to computers and the Internet primarily for educational purposes. All use of these resources must align with the educational goals of the College. Personal use of the network and devices is limited and must not interfere with the educational activities or the College's resources.

5. USE OF COLLEGE COMPUTERS IS A PRIVILEGE

Access to the College's computer systems and Internet resources is a privilege, not a right. Users must adhere to the guidelines set forth in this policy. Breaches may result in disciplinary actions, including:

- Access privileges suspension or revocation
- Monetary responsibility for repairs or damage
- Disciplinary actions
- Possible legal consequences depending on the severity of the breach.

6. UNACCEPTABLE USES

The following activities are prohibited on college computers and networks:

- **Pornographic & Offensive Material:** Accessing, downloading, or distributing sexually explicit, obscene, or lewd materials is prohibited.
- **Hate Speech & Harassment:** Transmitting content that promotes violence, discrimination, or harassment toward others.
- **Inappropriate Content:** Accessing or distributing material that does not align with the values of the College or is unrelated to educational goals, including un-Islamic content.
- **Personal Use:** Using College resources for personal entertainment, gaming, or downloading non-educational content.
- **Cyber Vandalism:** Attempting to disrupt, damage, or disable the College's systems, including spreading viruses, malware, or other harmful software.
- **Unauthorised Access:** Gaining access to restricted files, systems, or accounts without permission.
- **Privacy Violations:** Sharing or distributing personal information, including passwords, addresses, and other sensitive data.
- **Piracy:** Downloading, using, or distributing pirated software or engaging in any activity that violates copyright laws.

If unacceptable content is inadvertently accessed, the user must immediately notify the IT Department or Principal.

7. CONSISTENCY WITH OTHER SCHOOL POLICIES

All use of the College's computer systems must comply with the College's broader policies, including behavior policies, anti-bullying, and equality standards.

8. LIMITED EXPECTATION OF PRIVACY

- By authorising 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.
- 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.
- 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.
- 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.
- 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.

9. INTERNET USE AGREEMENT

- Before using the College's computer systems and Internet resources, users (students and staff) must sign an Internet Use Agreement form. Parents or guardians of students must also sign the agreement.
- The agreement confirms the understanding of this policy and acknowledges the responsibilities regarding acceptable use.

10. LIMITATION ON COLLEGE'S LIABILITY

The College does not accept responsibility for the loss, corruption, or damage of data on college computers or for service interruptions. Users must take appropriate precautions, such as regularly saving and backing up their data. The College is not liable for any financial consequences resulting from unauthorized use of its systems.

11. CYBER SECURITY

To protect against cyber threats, the College will implement the following:

Staff Guidelines:

- Use strong passwords and change them regularly.
- Lock devices when not in use.
- Refrain from sharing devices with students.

System Security:

- Regular testing and audits to identify vulnerabilities.
- Installation of anti-virus software and security patches.
- Restricting access to administrative systems to authorized personnel only.
- Conducting cybersecurity training for staff and students to raise awareness of potential threats.

Incident Response: In the event of a cyber-attack or breach, the College will follow an established incident response plan to contain, investigate, and resolve the issue which will include immediate notification to the Executive Principal / CEO.

Reviewed Date: [May 2025]
Approved by: [Executive Principal]
Next review: [May 2026]

APPENDIX 1: INTERNET USE AGREEMENT

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.

Student's Full Name (please print): _____

Student's 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: _____