

Rationale

At Ashdale Secondary College, we pride ourselves on using technology to further our students' educational learning environment. The College staff utilise research-based learning models to develop and support the ICT needs of all students. Ashdale Secondary College uses ICT as a tool for learning across the curriculum, which enables students to become competent, creative and productive users of technology and develop their knowledge, skills and capacity. This further enhances students' abilities to inquire, develop new understandings, create, and communicate with others to participate effectively in society, and prepare them for their lives beyond the College.

Definitions

'Information and Communication Technology (ICT)' means all computer hardware, software, systems and technology (including the internet and email) and telecommunications devices in facilities that may be used or accessed from the College campus or connected to the College's communication network. This includes all parent-funded and personal devices used on the College campus.

Principles

1. At Ashdale Secondary College, ICT is provided for educational purposes only.
2. Electronic devices are considered 'educational devices' and are not seen as rewards.
3. Students using the College's ICT must not break State or Federal laws (a summary of these laws are included in this Policy and form part of this Policy).
4. The College has the right to check all written, graphic, audio and other materials created, produced, communicated, stored or accessed on school ICT by students, including emails.
5. Students shall be made aware that access to ICT and, in particular, email and the internet can expose them to inappropriate material or potential harm.
6. Students shall take responsibility when using the College's ICT services by protecting their personal information and data, maintaining the required level of security, respecting the privacy of others, respecting the legal boundaries of licensing and copyright, using language appropriate to the College's expectations and taking good care of all ICT equipment.
7. Students shall take personal responsibility when using the College's ICT devices by protecting and ensuring all equipment is treated with respect.
8. The College will provide students with educational programs relating to cyber safety and appropriate ICT use.

Procedures

Ashdale Secondary College is committed to ensuring all students are aware of standards for the use of ICT within the College environment. Consequently, unacceptable use will not be tolerated under any circumstances, and disciplinary action will be taken against any student who breaches this policy as per the Ashdale Secondary College Student Engagement Policy.

Ashdale Secondary College shall identify acceptable and unacceptable use of ICT and is committed to regularly updating this policy.

1. Acceptable use includes:

- Taking notes in class;
- Researching information relating to assignments*; Gathering specific information about subjects/topics*;
- Using online websites or services as part of the curriculum;

- Completing online assessments;
- Emailing a teacher or friend for assistance with College-related work; and,
- Other teacher-directed activities.

**Students shall exercise caution regarding the quality and accuracy of the information they are accessing or transmitting.*

2. Unacceptable Use: includes but is not limited to:

- Accessing networks without College authorisation;
- Attempts to bypass the school network security/firewall whilst on the school network, such as through the use of a VPN;
- Vandalising or damage to any property owned or belonging to the College;
- Transmitting or deliberately accessing and/or receiving material that may be considered inappropriate, which includes threatening, sexually explicit, or harassing materials, offensive or discriminatory materials, or material that may be harmful either physically or emotionally, which includes bullying or harassment of fellow students or others outside the College. This includes filming and/or distributing footage of fights and/or physical altercations;
- Using Artificial Intelligence (AI) tools in a way contrary to learning or teacher directive, such as creating work and attributing it as their own;
- Communicating information concerning any password, identifying code or other confidential information or violating the security of the system in any way;
- Interfering with or disrupting network users, services or equipment, including unplugging or tampering with other school or students' devices. Disruptions include but are not limited to the distribution of unsolicited advertising or files, propagation of viruses in any form, "Jail Breaking" mobile devices and using the network to make unauthorised entry to any other machine accessible via your network;
- Plagiarising and/or breaching copyright laws, including software copyright and re-engineering of software;
- Conducting private business matters or using the system for any personal gain;
- Attempts to 'Air Drop spam' or send high volumes of unwanted content to other members of the College;
- Downloading and/or installing software programs (e.g. exe or pkg files) or apps without the permission of the College; and
- Inviting or accepting a College staff member to be a 'friend' on social networking sites (such as Facebook) or other learning management systems not managed by the College. ***Note: a page that a staff member manages on a site that is not managed by the College (e.g. wiki, or a private Blog) is acceptable as long as its' primary purpose remains education related.*

It is unlawful to send electronic messages, such as emails, which:

- Defame someone or an organisation;
- Infringe copyright laws, i.e. reproduce or adapt copyrighted material by downloading and further disseminating the material;
- Contain statements that could constitute sexual discrimination or sexual harassment;
- Display sexually offensive or explicit material.
- Contain offensive or insulting statements based on the race, colour, sexuality, gender or nationality of a person; and
- Undertake activities that breach State and Federal laws.

3. Electronic Computer Devices (excluding Phones):

Electronic computer devices include desktops, laptops, tablet computers and graphics calculators.

- Students are encouraged to use Electronic computer devices for educational purposes (see acceptable use).
- When used in a classroom, students must keep these devices inaudible unless directed by a teacher.
- Any damage found or accidentally caused to College devices must be immediately reported to the classroom teacher or school ICT Technicians.
- Personally-owned devices must meet the schools minimum BYOD device specification, specifically running up-to-date antivirus software.

4. Mobile Phones

- Students who bring mobile phones to the College are required to turn them off and place them in their bag from the first siren to the last siren of the day. It must remain off and in their bag during this time, including break times. This also applies to earpieces/ear pods.
- Mobile phones must not be connected to the school network or wireless.
- Smart watches are to be placed on aeroplane mode from the first siren to the last siren of the day.
- Emergency calls by parents are to be directed to Administration.

Devices may be confiscated and held in Student Services until the end of the day if used during school hours.

Unacceptable and/or unlawful use of ICT systems constitutes a breach of the College Code of Conduct and may warrant disciplinary action according to the Ashdale Secondary College Student Engagement Policy. Students must also be aware that the College may have to notify the Police or relevant authorities if an offence has been committed.

5. Personal Property Insurance

Parents/Guardians are encouraged to take out personal property insurance as the Department of Education does not cover the accidental loss, theft or damage of students' personal property. The College will not be responsible for the loss, theft, misuse, or damage of privately owned electronic devices or other valuables.

Email Use

At Ashdale Secondary College, students will use their education email for all College related correspondence with staff and the wider community for school education purposes only. This includes the use of Connect and any other College based communication tool. Emails should not be used for personal non-school purposes.

Student email address:

First name.surname@student.education.wa.edu.au

All students and parents should be aware that Ashdale Secondary College and the Department of Education WA may monitor student email. All students in Department of Education schools in Western Australia are required to undergo this filtering.

Internet Use

All network use on the school network is closely monitored. Any students abusing the available bandwidth will have their internet access revoked, ensuring access for everyone is responsive and fair.

The Department of Education and Ashdale Secondary College filters the internet for unsafe and inappropriate sites and blocks them from access. These filters are in place for the cyber security of the College network and safety of the students, and attempts to bypass these will be deemed to be in breach of this policy.

Students and parents should be aware that all internet traffic is monitored and logged, including attempts to bypass these measures.

When using any of the WA Department of Education's online services, students and parents agree:

- to the rules set out in the Acceptable Use Agreement;
- to give consent to the Department monitoring these services; and
- that any misuse of these services could result in disciplinary action.

Student Passwords

All students are issued with an account and password to access the College network, which should not be shared with others.

Your username and password provides access to:

- The Ashdale Secondary College network;
- Wireless connectivity for personally owned devices; excluding mobile phones
- College-owned computers (IT Labs and laptop trolleys);
- Connect; and
- Student email (First name.surname@student.education.wa.edu.au).

Students are responsible for the security of their account. Disclosing passwords leads to other users having access to student files, emails and any activity performed on the network will be logged against the incorrect student.

Students who use another student's password will be deemed to be in breach of this policy.

If a student suspects their password security has been breached, the student should immediately change their password when possible and report this occurrence to an ICT Technician or classroom teacher. A new password may be issued, and further misuse of the password will be monitored and dealt with as necessary.

Third-Party Service Providers Of Online Applications

Third-party online services are those provided by an external organisation, consultant or independent contractor and may be free or paid. Online third-party services often require separate account creation and login credentials and provide content, activities or transactions via the internet. These services often require Ashdale Secondary College to provide the personal information of students and/or parents.

Ashdale Secondary College will do its best to:

- identify third-party services which hold personal information for students;
- confirm a risk assessment of the Third Party Service Provider has been undertaken by the Department and a Third Party Service Risk Report is available; and
- implement the appropriate notification or consent option for an individual or their parent as specified in the Third Party Service Risk Report.

Legal Implications

Users are advised that the inappropriate use of electronic information can violate State and Federal laws. Please make yourself aware of the statutes that apply to your use of the College ICT facilities as indicated on the following page.

Important Statutes That Are Applicable To Students

Copyright Act 1968 (Cth)

Students may copy or otherwise deal with copyrighted material for the purpose of study or education. However, generally, only the author of the original material has the right to reproduce, copy, publish, perform, communicate to the public and make an adaptation of the copyrighted material.

Equal Opportunity Act 1984 (WA)

This Act precludes:

- Discrimination against persons on the grounds of sex, marital status or pregnancy, family responsibility or family status, sexual orientation, race, religious or political conviction, impairment or age in education;
- Sexual harassment and racial harassment in the workplace and educational institutions; and
- Promotes community recognition and acceptance of the equality of all persons regardless of their race, sexual orientation, religious or political convictions, impairments or ages.

Censorship Act 1996 (WA)

Students must not use a computer service to transmit, obtain or request an article knowing that it contains objectionable and restricted material. It is an offence to possess or copy indecent or obscene articles or child pornography. Students should be aware for their own protection that people who deal with such material commit an offence.

Criminal Code (WA)

Students should be aware that it is illegal to show offensive material to children under 16 and that if someone does show them offensive material, that person is committing an offence. Racist harassment and incitement to racial hatred are also criminal offences.

Cybercrime Act 2001 (Cth)

Unauthorised access to or modification of data held in a computer and unauthorised impairment of electronic communication e.g. 'hacking' or infecting computer systems with a virus, is illegal.

Privacy Act 1988 (Cth)

Students should respect that the personal information of others is private. This Act covers the collection, use and disclosure, quality and security of personal information.

Online Safety Act (2021)

Legislation regulating issues including cyber-bullying, cyber-abuse and image-based abuse or online content.