AVELEY
SECONDARY COLLEGE

Information and Communication Technology Policy

2023

Contents

Parents and Carers

Rationale

Information and Communication Technology (ICT) is utilised in schools for learning, teaching and administration. The availability of such resources provides the opportunity for schools to help students develop their full potential. ICT provides significant educational value but can pose risks regarding safety, personal and corporate reputation.

Bring You Own Device (BYOD) has been implemented at Aveley Secondary College (ASC) to allow students access to their personal devices for educational purposes to enhance motivation and engagement within a classroom setting. Our aim is to prepare students to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. We recognise that ICT is an important tool in both the society we live in and in the process of teaching and learning. Students use ICT tools to find, explore, analyse, exchange and present information responsibly and creatively.

This policy document sets out the school's rationale, principles and strategies for the delivery of Information and Communication Technology. Students will learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of people, communities and cultures. Increased capability in the use of ICT promotes initiative and independent learning. Students will be able to make informed judgements about when and where to use ICT to best effect and can consider its implications for home and work, both now and in the future.

Principles

- This policy concerning student use of ICT shall reflect the teachings and educational goals of the school. The usage of ICT shall be balanced with all elements of the school curriculum.
- ASC shall ensure policies and practices are effective in ensuring appropriate usage by students of ICT.
- All written, graphic, audio and other materials created, produced, communicated, stored or accessed on school ICT and privately owned ICT being used on the school site, including emails, are the property of the school, and as such, are subject to monitoring by the school.
- ICT is provided to students as a tool to support learning and as such should be used in accordance with the expectations of the school as set out in this policy.
- The use of the school, student and family-owned ICT on the school site, including the internet, email, and social media by students shall not be contrary to relevant State and Commonwealth laws, a breach of school rules or policy, or otherwise be inappropriate or offensive.
- As parents/caregivers are the prime educators of their child, they shall be informed of the school policy and encouraged to assist in facilitating its implementation.

1:1 BYOD iPad Program

iPad General Use

- Students are responsible for all information and content on the device, which should adhere to this Acceptable Use Agreement guidelines for ICT as signed on enrolment.
- The iPad should come to school each day with 100% charge for the day's activities.
- The iPad must not be left unattended at any time, the device's safety is the responsibility of the student. It is the student's individual responsibility to ensure that the iPad is looked after.
- iPads must be secured in a high-quality protective case.
- Like all personal items brought to school, the school has no liability for damage or loss of any personal items brought to school.
- The iPad must be always used under the direction of the teaching staff. Misuse will result in the temporary removal of the device.
- BYOD devices are used and connected to WIFI subject to the device having Zuludesk Management Software installed unless another arrangement has been agreed to.
- The websites and apps used on the iPads while at school are subject to third-party consent policies.

iTunes

- An iTunes account is necessary to download applications (software) to allow the iPad to function. See the Apple ID and Family Sharing Guide for instructions to create an iTunes Account and an Apple ID.
- Parents/Legal Guardians may need to purchase a $50 iTunes voucher for the purchase of core educational apps from the iTunes Store (as outlined in the Contributions and Charges).
- By using the iTunes software, a user agrees to be bound by the terms and conditions of the Software Licence Agreement.
- By using the iTunes Store website, a user agrees to be bound by the Terms and Conditions of Use that apply to the website.
- The user is entirely responsible for maintaining the confidentiality of information held in their account, including their password and for any activity that occurs under their account as a result of failing to keep this information secure and confidential.
- It is highly recommended that the iPad setup process is followed carefully (See Apple ID and Family Sharing Guide)

iPad Restrictions

We strongly suggest that parents/guardians look at the restrictions area in the iPad settings. It would be appropriate to enable restrictions to the section at the bottom of the menu for the "Allow Content". This can be made appropriate for the Senior School age group for the different categories. The passcode should not be known by the student.
Zuludesk will restrict the visible apps on the iPad while connected to school WIFI and during school times, to apps deemed necessary for school use. Outside of these times, all other apps will appear, and restrictions will cease.

Cloud Storage

It is important to note that we will be using Google Suite for Education as well as some other programs and apps that use cloud-based storage. iCloud will be used to back up student iPads, instructions are provided by ASC, and school staff have no access to iCloud data or passwords.

ICT Management

The Teaching and Learning Coordinator will, with the assistance of the ICT Committee and Network Administrator, facilitate the use of Information and Communication Technology in the following ways:

- By updating the ICT policy and scheme of work
- By ordering/updating resources
- By keeping staff abreast of new developments
- By ensuring that opportunities occur for students to develop ICT capability and that progression is taking place
- Supporting staff in developing students' capability
- Contributing to the School Improvement Plan on an annual basis
- The Network Administrator will communicate problems to the school leadership
- Making sure all staff understand the system for logging faults and use of the Internet/email
- Maintaining records of software licences and their deployment
- Provide appropriate content on the school intranet for use by staff and students
- Maintain regular backups of user and shared data.

Access to ICT

Network access

Staff and students have access to reliable and industry-standard hardware and software in order to use ICT effectively as a teaching and learning resource, and as a working tool for management and administration. Digital Technologies Labs are equipped with Windows Desktops Computers with up-to-date software and hardware.

All staff and student users have access through the school's network to their H Drive as well as shared drives. All staff and students have access to a Google Drive account to save and access school/educational documents.

Staff and Students should not load software onto network machines. Software licences need to be investigated and approved before being loaded onto machines.

Computers for student use

The teaching of ICT is mandated via Digital Technologies and therefore these classes are the only labs with access to desktops for student use due to the school BYOD policy. A policy of integrating ICT into teaching and learning across the curriculum is reflected in the ongoing provision of digital projectors and Apple TVs in each classroom.

Monitoring and Review

Monitoring of the Network and ICT Usage is carried out by the Network Administrator in the following ways:

- Informal discussion with staff and pupils.
- Analysis of ICT Dashboard and FortiGate data.
- Analysis of student and shared network files.
- Monitor user quotas and warn users of excessive usage.
- Investigate excessive use and inappropriate sites and files.
- Block inappropriate sites using the web filter.
- Report inappropriate usage and enforce bans where appropriate.

Handling ICT Concerns

Parents, teachers and students can submit a complaint directly to student services regarding ICT complaints or concerns. Prompt action will be undertaken if a complaint is made. The facts of the case will need to be established. For example, it is possible that the issue has arisen through home Internet use or by contacts outside school. Transgressions may be of a minor or potentially significant nature. Sanctions for irresponsible use will be linked to the school's behaviour/disciplinary policy.

If staff or students discover unsuitable sites, the URL (address) and the content will be reported to the Network Administrator. The Network Administrator will immediately prevent access to any site considered unsuitable. Where appropriate an investigation will be undertaken, and appropriate action will be taken.

- Parents and students will need to work in partnership with student services to resolve any issue
- The student may have electronic communication access or computer access denied for a period.

Critical E-Safety incidents

A critical e-safety incident is when unlawful or suspected unlawful material is found on any computer or digital device where criminal or inappropriate activity has or is taking place, or where an e-crime or unlawful act has been or is being committed. In such cases, the power lead should be taken out (not a normal shutdown) or the battery removed (laptop) or the device confiscated (iPad/Mobile devices). Do not show (suspected) unlawful material to anyone else or undertake any further investigation, report to the Principal Immediately. Notes should be made that help in any subsequent local or police investigations

Students

Acceptable Use

Acceptable use shall include, but is not limited to:

- Gathering, organising, creating and sharing appropriate information for educational or related purposes.
- Encouraging collaborative projects and resource sharing.
- Any other tasks that are for educational purposes or that support and promote the school and its ideals.

Cyber-safety: Prevention and Response

- Students are to be supervised when using devices.
- iMessages and social networking apps (e.g., Facebook, Snapchat, Instagram, TikTok) are restricted on the school network. Any student found to be using these apps or viewing saved content from restricted sources within the school will be logged and the Student Services Manager notified. Appropriate actions may include loss of ICT privileges.
- Any incident between students out of school should be reported to student services.
- Students are encouraged to take screenshots as evidence.
- All teaching staff are expected to follow the DET Social Media Policy.
- Parents found to be using social media in a discriminatory way against a teacher or student will be followed up by the leadership team.
- All staff will be notified of any areas to be concerned about in relation to cyber safety.
- All Passwords are to be kept securely.

Unacceptable Use

Unacceptable use shall include but is not limited to:

- Accessing networks without proper authorisation, including hot-spotting and VPN.
- Transmitting or deliberately accessing, creating and/or receiving material that is inappropriate or offensive. Inappropriate or offensive material includes but is not limited to threatening, sexually explicit, offensive, defamatory or discriminatory materials, or material that may be harmful physically or emotionally, including bullying or harassment within or outside the school.
- Unauthorised disclosing or communicating of information concerning any password, identifying code or other confidential information without written permission.
- Interfering with or disrupting network users, services or equipment. Disruptions include but are not limited to unsolicited advertising, intentional propagation of viruses in any form and using the network to make unauthorised entry to any other machine accessible via the school network (i.e., ‘hacking’).
- Using school network and/or equipment to conduct private business for commercial gain or promote material unrelated to school-defined tasks.
- Logging on to the network with another user's account or sharing another account.
- Tampering physically with the equipment.
- Installing software or files without authorisation.
- Headphones during class without teacher direction.

Unlawful Use. (E-crimes)

Unlawful use shall include but is not limited to:

- Defaming a person or organisation in an email, web page or through social media.
- Infringing of copyright laws i.e., reproduction or adaptation of copyrighted material by downloading and further disseminating the material.
- Digital communication could constitute sexual discrimination or sexual harassment.
- Digital communication could constitute cyberbullying.
- Storing, accessing, displaying or creating sexually offensive material.
- Sending digital communications which are discriminatory on the basis of, for example, race, sex, gender, disability or age.
- Undertaking activities that breach State or Commonwealth Legislation.

Consequences

Students who breach the school's ICT policy may be subjected to the following consequences;

- Warning and advice on incorrect behaviour.
- Classroom teachers will log any breaches.
- Parent/Guardian communication may occur regarding the breach.
- Parents/guardians will be invoiced for repairs to any vandalised/damaged equipment.
- Devices used inappropriately will be confiscated and returned at the end of the day.
- Inappropriate websites and applications will be blocked.
- Behaviour consequences are escalated to the Head of Learning Area, Student Services or Administration as appropriate
- Unlawful use can be reported to the police.

Staff

Management and Maintenance of Devices for Staff

- Any issues with school-owned computers/iPads/Apple TVs must be noted in writing to the Network Administrator who will then arrange for the appropriate maintenance work, this does not apply to student iPads.
- Staff should not take any school devices to external maintenance.
- Maintenance will be carried out at the earliest possible convenience.
- Staff and students are expected to ensure that they use the devices in a manner that reduces the risk of any incident that may cause damage occurring to a device.
- All electrical cords must be tested each year, arranged by Spotless.
- All devices are expected to be locked away securely and charged ready for use.
- Laptops under the NFT program are to be logged with the Helpdesk for maintenance and management issues.

Staff issues

All staff are entitled to training to improve their ICT capability and are responsible for keeping abreast of ICT developments. The ICT Coordinator or Learning Area ICT Leader can be contacted to request support and training in the use of ICT.

References

Copyright Act 1968 (Cth)
Students may copy or otherwise deal with copyright 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 copyright material.

Equal Opportunity Act 1984 (WA)

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. Possessing or copying indecent or obscene articles or child pornography is an offence. Students should be aware for their own protection that people who deal with such material commit an offence.

Classification (Publications, Films and Computer Games) Enforcement Act 1996

Criminal Code Act (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, are 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.

Links to Policies
DET: Department Online Services for Parents
http://det.wa.edu.au/policies/detcms/policy-planning-and-accountability/policies-framework/guidelines/department-online-services-for-parents.en?cat-id=3457966

DET: Students Online Guidelines
http://det.wa.edu.au/policies/detcms/policy-planning-and-accountability/policies-framework/guidelines/student-online-guidelines.en?cat-id=3457121

DET: Students Online Policy
http://det.wa.edu.au/policies/detcms/policy-planning-and-accountability/policies-framework/policies/students-online-policy.en?cat-id=3457121

DET: Telecommunications Use
http://det.wa.edu.au/policies/detcms/policy-planning-and-accountability/policies-framework/policies/telecommunications-use.en?cat-id=3457966

DET: ICT Security Policy and Procedures
http://det.wa.edu.au/policies/detcms/policy-planning-and-accountability/policies-framework/policies/information-and-communication-technologies-security-policy-and-procedures.en?cat-id=3457966