

# DARA SCHOOL

35  
INFORMATION AND  
COMMUNICATION  
TECHNOLOGY POLICY

## INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

### 1. PURPOSE

Dara School provides a significant level of information and communication technology (ICT) to enhance teaching and learning and contribute to the academic and social development of the students. The primary purpose of ICT at Dara School is to promote educational excellence by facilitating innovation and communication.

ICT includes the provision of hardware, software and access to the Internet. The Internet is a global network that enables access to a wide range of information sources and communication opportunities including email.

This policy covers the utilisation of any equipment, property or resource at any time, whether during or outside of school hours, and includes the use of remote access facilities. Further, this policy also applies to the use of personal devices accessing Dara School's resources.

### 2. SCOPE

This policy, from the date of endorsement, applies to all people involved in Dara School. This includes:

- Dara employees (permanent and casual),
- Students,
- Parents and Caregivers,
- Volunteers,
- Contractors,
- Sub-contractors,
- Work experience students,
- Indirect service providers,
- Any other individual involved in this organization.

### 3. POLICY PRINCIPLES

In alignment with the National Safe Schools Framework, Dara School is committed to:

- Affirming the rights of all members of the school community to feel safe and be safe at school,
- Acknowledging that being safe and supported at school is essential for student wellbeing and effective learning,
- Accepting responsibility for developing and sustaining safe and supportive learning and teaching communities that also fulfil a school's child protection responsibilities,
- Encouraging the active participation of all school community members in developing and maintaining a safe school community where diversity is valued,
- Actively supporting young people to develop understanding and skills to keep themselves and others safe,
- Developing a safe school community through a whole-school approach.

In addition to the above, Dara School looks to undertake the following practices with use of information and communication technologies:

- Have in place Acceptable Use of ICT Agreements (R-4, 5-12 and Adult),
- Ensure that users use information and communication technologies in a safe and responsible manner,
- Ensure that users follow the copyright and licensing laws with respect to software, information and other material retrieved from or published on the Internet,
- Make children and students aware of the importance of ICT security and safety, and how to properly react and deal with ICT security incidents and weaknesses.

#### 4. THE RESPONSIBLE USE OF ICT

The school computer network and other communication facilities are educational and business facilities provided by the school to be used primarily for educational purposes. All users, therefore, have a responsibility to use these resources in an appropriate, ethical, safe and lawful manner.

When individuals choose to go public with opinions via blogs, a social networking site or personal website, they are legally responsible for their commentary. Individuals can be held personally liable for any commentary deemed to be defamatory, obscene, proprietary or libelous. Users should exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, derogatory remarks or characterisations.

Users should also consider the information and images of them available on their sites and make sure that they are confident these are appropriate representations of their character.

Sexual harassment or acts that amount to criminal or sexual assault may be referred to the police. Anyone who has been subject to such an act may take legal action. Acts that constitute an e-crime will be referred to SAPOL. Acts where there is suspicion of child protection issues must be referred to the Child Abuse Report Line (13 14 78) in line with mandatory reporting requirements.

#### 5. MOBILE PHONES AND ASSOCIATED DEVICES, SUCH AS SMART WATCHES.

Dara School does not allow student use of personal communication devices such as mobile phones or smart watches during School hours and OSHC services.

#### 6. BRING YOUR OWN DEVICE (BYOD)

Students, along with staff and visitors, may bring a personal device from home for educational use. The school holds no responsibility for these devices. However, if a user wishes to use a personal device then the following conditions must be adhered to:

- Up to date antivirus software must be installed and maintained,
- All updates to operating systems must be accepted and installed regularly,
- Devices must be brought to school fully charged,
- Only staff devices may be charged on-site and only if they comply with Tag and Test requirements in accordance with our Electrical Safety policy,
- Insurance cover is the user's responsibility for any personal device brought to school.
- All users, when connected to the school network, will be directed through the school's internet filtering and monitoring system.

#### 7. INTERNET USE

Use of the internet is intended for research and learning and communication between students and staff. Responsible use of the services by all users is an expectation of the school to ensure a safe learning environment.

The internet provides an opportunity to enhance students' learning experiences by providing access to vast amounts of information across the globe. Access to internet tools at school will assist students to develop the information and communication skills necessary to use the internet effectively and appropriately.

#### 8. INTELLECTUAL PROPERTY, COPYRIGHT AND ACADEMIC INTEGRITY

All users of Dara School's ICT infrastructure are reminded of their responsibility to respect the intellectual property of others. Staff and students are covered by a remuneration notice with the Copyright Agency and can rely on the statutory license to copy and communicate text, images and notated music subject to certain conditions. For information, please visit the [Australian Copyright](#)

[Council](#). In addition to the statutory license, other provisions in the Copyright Act permit educational institutions to use copyright material without permission from the copyright owner. These include section 200AB (the “special case” or “flexible dealing” exception) and section 28 (playing music and showing films in class). These exemptions do not exist outside of the work students and staff complete at school. As such, students will be taught the skills to operate both inside and outside of the statutory agreement.

## **9. ELECTRONIC COMMUNICATION**

The ease and immediacy of electronic communication makes it an attractive form of communication; however, electronic communication has its limitations and drawbacks. Students should exercise good judgement and common sense when creating and distributing messages. The school and/or individuals may be liable for defamatory, misleading or deceptive statements contained in messages, and may also be liable for the disclosure of information which is confidential, or which constitutes personal information as defined by the Privacy Act 1988 (Cth).

## **10. ROLES AND RESPONSIBILITIES**

### **PRINCIPAL**

- Review this policy regularly, ensuring it meets legislative requirements.
- Develop a school learning environment which is safe and inclusive of learning.
- Inform the school community of the expectations of this policy and ensure a copy is included in the enrolment pack. A copy of the policy is also available through the school’s community communications platform.
- Ensure all users of the school’s network sign ICT user agreements.
- Provide professional learning opportunities for staff to gain knowledge, understanding and skills in enhancing student learning.
- Facilitate the involvement of other agencies to support ICT resources and use in the School and OSHC service.
- Adhere to the Acceptable Use of ICT Agreement – Adult.

### **ICT ADMINISTRATOR**

- Review user statistics and filtering tools, involving ICT support to block access to inappropriate sites and filter specific words and phrases that could be used for inappropriate searches or messages where necessary.
- Maintain and update the network’s anti-virus software.
- Manage and monitor user accounts and network use.
- Inform the Principal of any instances of misuse of the internet, email service, or other ICT equipment.
- Ensure the school’s web filter is up to date, effective and maintained.
- Ensure that the software installed by the school is covered by the necessary licenses.
- Adhere to the Acceptable Use of ICT Agreement – Adult.

### **TEACHERS**

- Adhere to this policy and refer any questions to appropriate channels.
- Monitor the activity of students in the classroom.
- Ensure students are aware of the expectations of this policy by facilitating student ICT agreements by the end of the first week of the student’s enrolment.
- Discuss the contents of this policy before permitting students to use ICT facilities, regularly reminding students of the contents of the user agreement they have signed, and encouraging them to make positive use of ICT.
- Develop students’ ICT skills and knowledge:
  - Teach students how to access and use the ICT equipment correctly.
  - Guide students in effective strategies for searching and using the internet.
  - Provide explicit cyber-safety instruction as outlined in school curriculum documents.

- Provide adequate supervision for students while accessing ICT.
- Observe copyright laws and educate students to correctly reference works.
- Follow up on and report breaches of this policy as soon as practicable.
- Adhere to the Acceptable Use of ICT Agreement – Adult.

#### **SCHOOL SUPPORT STAFF**

- Support the supervision of student use of ICT.
- Adhere to copyright and intellectual property laws and cyber safety principles.
- Adhere to the Acceptable Use of ICT Agreement – Adult.

#### **OSHC STAFF**

- Supervise student use of ICT when in OSHC.
- Ensure students do not access school devices during OSHC. Only personal devices, including BYOD, are allowed.
- Adhere to the Acceptable Use of ICT Agreement – Adult.

#### **STUDENTS**

- Use ICT in the appropriate manner and follow guidelines.
- Adhere to copyright and follow cyber safety principles.
- Students who are not following the guidelines that have been outlined in the user agreement may have their device confiscated until it can be returned to a parent at the end of the day,
- Students using the internet have the responsibility to report inappropriate behaviour and material to their teachers.
- Students who bring their own device (BYOD) must ensure they are charged and ready for use. No charger cables are permitted at school. Power banks are permitted.
- Students' devices will be directed through the school's internet filtering and monitoring system, to ensure safety and appropriate use.

#### **PARENTS**

- Discuss positive ICT use with their child.
- Support the school's cyber-safety program by emphasising the need to follow cyber-safety strategies.
- Contact the principal or delegate to discuss any questions and/or report any breaches about cyber-safety and/or this policy.
- Cover the cost of damages to ICT that their child has caused.
- Support the ethos of the school by modelling a positive online presence.
- Will ensure students who bring their own device to school (BYOD), bring a fully charged device and do not bring a charger cable as these are not allowed in accordance with our Electrical Safety policy.
- Agree to the school installing security software to enable safe use on BYOD (as applicable to all school devices).

### **11. MONITORING, EVALUATION AND REVIEW**

The effectiveness of the Policy will be monitored and evaluated in relation to the following:

- Ongoing data will be collected within the school to inform the monitoring and evaluation process, and this will lead to further review of the policy,
- School leaders will provide ongoing support monitoring of the School's compliance with this policy,
- The policy is to be reviewed every 5 years by School leadership.

### **12. DEFINITIONS AND ABBREVIATIONS**

**User** Any person using the information technology facilities.

**Information and Communication Technology (ICT)** includes the systematic application of computing,

	telecommunications, media and other electronic technologies to the collection, processing, transformation, organization, storage, transfer, and presentation of information in all its forms, to enhance the performance of individuals in all school activities.
<b>Administrator</b>	The person appointed by the School as having responsibility for the security and management of all or part of Dara School's information technology facilities.
<b>A safe and supportive school</b>	'In a safe and supportive school, the risk from all types of harm is minimized, diversity is valued, and all members of the school community feel respected and included and can be confident that they will receive support in the face of any threats to their safety and wellbeing.' National Safe Schools Framework, updated 2013, Education Services Australia.
<b>Parent</b>	Natural parents, legal guardians, and caregivers.
<b>Cyber-safety</b>	The safe use of the Internet and ICT equipment/devices, including mobile phones.
<b>Inappropriate material</b>	This means material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school environment.
<b>Personal use</b>	This means all non-work-related use, and includes internet usage and private emails.
<b>BYOD</b>	Bring Your Own Device is a program in which students bring personally owned devices to school that are managed by the school so that they can be used for school learning activities.

### 13. DISCLAIMER

The school accepts no responsibility for any damage or loss arising directly or indirectly from the use of any ICT service or infrastructure or for any consequential loss or damage. The school makes no warranty, expressed or implied, regarding the services/facilities offered or their fitness for any particular purpose.

The School will not be responsible for the loss of any data or software stored in the Information Technology Facilities. Although standard back-up procedures may be in operation on some Information Technology facilities, the user is responsible for the maintenance of copies of any data or software controlled by the user.

A commercial filter is used on the internet connection to prevent access to inappropriate sites. However, no guarantee can be made that new sites will be blocked immediately.

Electronic communication is not a secure means of communication. While every attempt would be made by Dara School to ensure the security of its resources, users must be aware that their security is not guaranteed, particularly when communicated to an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

### 14. BREACHES TO THE POLICY

The school will be vigilant in managing use of resources to improve learning outcomes. Misuse of ICT such as desktop computers, laptops, notebooks, tablets, digital cameras will be dealt with according to the nature of the infringement.

Breaching the conditions stated in the Acceptable Use of ICT Agreement may result in disciplinary action, which may include restriction or withdrawal of access to digital resources.

## 15. SUPPORTING DOCUMENTS

- Wellbeing Policy 22
- Privacy and Confidentiality Policy 23
- Child Protection Policy 1
- Copyright Policy 31
- Electrical Safety Policy 28

## 16. FORMS ASSOCIATED WITH THIS POLICY

35.1	Guidelines
35.2	Strategies to help Dara Students Cyber-Safe
35.3	ICT User Agreement (R-4) Junior
35.4	ICT User Agreement (5-12)
35.5	ICT User Agreement Adults

## 17. EDUCATION STANDARDS BOARD

This policy supports criterion 3.4 of the Standards for Registration and Review of Registration of School in South Australia.

*Criterion 3.4                      The school implements policies and procedures for student welfare that covers pastoral care, early intervention, child protection including mandatory reporting and behaviour management including associated safety and wellbeing management.*

## 18. EDUCATION STANDARDS BOARD

This policy supports criterion 3.4 of the Standards for Registration and Review of Registration of School in South Australia.

Title	Information and Communication Technology (ICT)
Policy Reference Number	35
Responsible for review	School Leadership
Implemented	25 June 2019
Reviewed	March 2023
Reviewed	July 2023
Policy due for Review	March 2028