INFORMATIONS & COMMUNICATIONS TECHNOLOGY (ICT) POLICY

Eudunda Area School

Students at Eudunda Area School are encouraged to use ICT (Information Communication Technology) for supporting and developing their education and learning the essential skills of becoming a digital citizen. Access to the school's computers, internet and services depends on students acting in accordance with the conditions set out in this Acceptable Use Policy.

The overall goal of Eudunda Area School is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. This Use Policy includes information about obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

This Acceptable Use Policy is a combination of Department for Education and Eudunda Area School policies and covers four key areas: School specific ICT information, Cyber Safety, Learnlink Office 365 and BYOD (Bring Your Own Device). **By signing the Eudunda Area School ICT & Cyber Safety User Agreement, you are agreeing to the terms laid out in this document.**

Students are not permitted to use school ICT equipment and services until both students and parents/caregivers have signed and returned the Agreement Form to the school (a one week grace period applies for new enrolments).

Students are expected to use the ICT facilities for educational related purposes only. Students can assume that their actions and files when using any computer in the school may be logged and monitored at any time, this includes (but not limited to) any stored content, internet use and e-mail. Files stored in their personal folders are not considered private (except from other students).

Where a student is suspected of an electronic crime, this will be reported to the South Australia Police. Where a personal electronic device such as a mobile phone is used to capture images of a crime, such as an assault, the device will be confiscated and handed to the police.

While every reasonable effort is made by schools and The Department for Education administrators to prevent student's exposure to inappropriate content when using the Department's online services, it is not possible to completely eliminate the risk of such exposure. In particular, the Department cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. The Department recommends the use of appropriate Internet filtering software.

More information about Internet filtering can be found on the websites of the Australian Communications and Media Authority at http://www.acma.gov.au, NetAlert at http://www.netalert.gov.au, the Kids Helpline at http://www.kidshelp.com.au and Bullying No Way at http://www.bullyingnoway.com.au. Please contact the principal, if you have any concerns about your child's safety in using the Internet and ICT equipment/devices.

Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices for themselves and the people around them regardless of the time of day. Being cyber-safe is no exception and we invite you to discuss with your child the following strategies and expectations to help stay safe when using ICT at school and after formal school hours.

INFORMATIONS & COMMUNICATIONS TECHNOLOGY (ICT) POLICY

Eudunda Area School

ICT & Cyber Safety Student Expectations:

1. I will only log on with my username and not allow anyone else to use my account.
   - I will keep my password private. I will not write down or tell my password to another person.
   - I will not let another person see me enter my password.
2. I will not attempt to gain unauthorised access to any computer system or other users account.
3. I will not attempt to bypass any hardware and/or software protection systems.
4. While at school, I will:
   - access, attempt to access, download, save and distribute only age appropriate and relevant material.
   - report any attempt to get around or bypass security, monitoring and filtering that is in place at school.
5. I will use the ICT equipment only for positive purposes, not to be mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the school itself, even if meant as a joke.
6. While at school or a school related activity, I will inform the teacher of any involvement with any ICT material or activity that might put me or anyone else at risk (eg bullying or harassing).
7. If I accidentally access inappropriate material, I will:
   - not show others.
   - turn off the screen or minimise the window and report the incident to a teacher immediately.
8. To ensure my compliance with copyright laws, I will download, store or copy files such as music, videos, games or programs only with the permission of a teacher or the owner of the original material. If I infringe the Copyright Act 1968, I may be personally liable under this law.
9. My privately owned ICT equipment/devices, such as a laptop, mobile phone, USB/portable drive I bring to school or a school related activity, are also covered by the ICT and Cyber Safety User Agreement. Any images or material on such equipment/devices must be appropriate to the school environment.
10. I will ask my teacher's permission before I put any personal information online. Personal identifying information includes any of the following: my full name, address, email address, phone number, photos of me and/or people close to me.
11. I will not use the computer systems for any form of cheating or plagiarism.
12. I will respect all school ICTs and will treat all ICT equipment/devices with care. This includes:
    - not intentionally disrupting the smooth running of any school ICT systems.
    - not attempting to hack or gain unauthorised access to any system.
    - reporting any breakages/damage to a staff member.
    - not behaving in a way that might damage ICT equipment (including eating/drinking in computer areas).
13. The school may monitor traffic and material sent and received using the school's ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including e-mail.
14. I will follow any reasonable instruction from a staff member where they consider my use of ICT to be unacceptable or inappropriate.
15. If I do not follow cyber-safe practices, the school may inform my parents/caregivers. In serious cases, the school may take disciplinary action against me. My family may be charged for repair costs. If

illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform the police and hold securely personal items for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.

BYOD (Bring Your Own Device)

All students are expected to have a device for school use. This is to ensure that all students have equal opportunity to develop ICT capabilities and digital literacies. These skills are embedded throughout the Australian Curriculum and are important to success in our modern world.

Devices may be purchased via the EAS Recommended Device Portal, or from a retail supplier of your choice.

Software: All software required for learning is made available through the school and covered by school fees. No additional software is required when purchasing a device. For detailed information about BYOD, our BYOD Recommended Device Portal or how to get started visit http://EudundaAS.technologyportal.com.au

Charging Devices & Electrical Testing

Students can charge their batteries if they are running low however the device and charger must be electronically tested and tagged to comply with Workplace, Health and Safety Act 2012 and related regulations and standards.

Loss of Data

The school accepts no responsibility for loss of data, due to user error, hardware and software failure or otherwise. We recommend student's backup their work to multiple locations, such as a USB flash drive, home computer and/or OneDrive – free student Cloud storage.

Student Email

Students at this school are provided with a Learnlink (Office 365) school email account. Outside accounts such as Gmail and Hotmail are not permitted. Students are able to access their school email from home.ICT & Cyber Safety Acceptable Use Policy

LearnLink Office 365

LearnLink Office 365 for education provides students with an email and collaboration platform to create and/or upload/share content. This may include websites, presentations, written, audio, images and video material as part of their educational program. This includes Email and Office Online (Word, PowerPoint, Excel, and OneNote). Each student will receive also 1 Terabyte of storage space in Microsoft's Australian Cloud. By default all data and files are private, however they can be shared with other LearnLink Office 365 users, including staff and students of other schools, but not anyone external to the Department. Online data is stored off-site in Australia by Microsoft (the Australian & US government has access to the data through enquiry).

It is also possible for students to download a copy of Office 365 ProPlus to install on their personal device. ProPlus applications can be installed on up to 5 personal devices owned by a student. Once installed, the applications can be used without an internet connection. Periodic internet connection is required for accessing data stored in cloud services, updates and licencing via your LearnLink Office 365 account.

It is recommended personal devices have suitable anti-virus/anti-malware software installed and regularly updated, and the device operating system is regularly updated. Users of LearnLink Office 365 are responsible for the information/data in their LearnLink Office 365 account including OneDrive, OneNote and email; any important information should be backed up. This account must not be used to store or share sensitive or personal information. If a parent or student wishes to opt out of using this product, they may notify the school in writing.

Breach of the Acceptable use policy

Eudunda Area School reserves the right to withdraw services from students if they are in breach of this acceptable use policy or if computing facilities are generally misused, and to take other disciplinary action against individual students who misuse computing facilities. Students may be required to pay for wilful or accidental damage caused to school computers, hardware or equipment.

Administrators reserve the right to examine, use and disclose any data found through investigation to relevant authorities (eg school administration/police).

By signing the Eudunda Area School ICT & Cyber Safety User Agreement, you are agreeing to the terms laid out in this document.

This policy will be reviewed as part of the school's three-year review cycle. Ratified 1st April 2026