**­**

***Kangaroo Inn Area School***

Strive for Life

Principal: Annie Matthews & Amy Oswald

PMB 24

Millicent SA 5280

School No: 0957

Ph: (08) 8734 3046

Fax: (08) 8734 3134

Email: dl.0957.info@schools.sa.edu.au

****­

**Kangaroo Inn Area School ICT Acceptable Use Agreement**

Dear Parent/Caregiver,

The measures to ensure the cyber-safety of Kangaroo Inn Area School are based on our core values. To assist us in enhancing learning through the safe use of information and communication technologies (ICTs), we are now asking you to read this document and sign the attached Use Agreement Form.

Rigorous cyber-safety practices are in place, which include Cyber-Safety Use Agreements for staff and learners. Child protection education, such as the Keeping Safe child protection curriculum, includes information about remaining safe when using new technologies and is a mandated curriculum program for all learners.

The computer network, Internet access facilities, computers, and other ICT equipment/devices bring great benefits to the teaching and learning programs at Kangaroo Inn Area School, and to the effective operation of the school. The ICT equipment is for educational purposes appropriate to this environment, whether it is owned or leased either partially or wholly by the school, and used on or off the site.

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

All learners will be issued with a Use Agreement, and once signed consent has been returned to the school, learners will be able to use the school ICT equipment.

Material sent and received using the network may be monitored, and filtering and/or monitoring software may be used to restrict access to certain sites and data, including e-mail.

While every reasonable effort is made by schools, preschools, and Department for Education (DfE) administrators to prevent children’s exposure to inappropriate content when using the department’s online services, it is not possible to eliminate the risk of such exposure. DfE cannot filter Internet content accessed by your child from home, from other locations away from school, or on mobile devices owned by your child. DfE 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](http://www.acma.gov.au/), NetAlert at [http://www.netalert.gov.au](http://www.netalert.gov.au/), the Kids Helpline at [http://www.kidshelp.com.au](http://www.kidshelp.com.au/), and Bullying No Way at [http://www.bullyingnoway.com.au](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.

Additional Points from the Department for Education:

1. Students must only use their own assigned computer network accounts.
2. Students must not share personal information about themselves or other students with third parties, including their username or passwords.
3. Students must not engage in chats or other communication with third parties except when done so as part of curriculum learning.
4. AI software and websites should be used in an appropriate manner and not used for plagiarism or the creation of inappropriate or offensive content.
5. Personal information should not be entered onto websites that are not endorsed by the department, including writing aid, AI, and chat websites (excluding EdChat).
6. School ICT assets must not be used to access or share inappropriate content online, including sexually explicit materials, obscene depictions, harmful materials, illegal activities, profane or abusive language, or content that others may find offensive.
7. Web and email content filtering must not be circumvented to access content that has been deemed inappropriate for students.
8. Software designed to circumvent web and email content filtering or other security controls must not be installed or used on devices. This includes unapproved VPN software, proxy websites, hacking tools, or the use of built-in device functions to bypass security controls.
9. Hacking, cheating, and plagiarism tools must not be installed or used on devices. This includes software that gives users an unfair advantage in games or other activities.
10. Copyright materials (including games and movies) must not be illegally downloaded onto or accessed using school or department-issued ICT assets.
11. When using online communities, users must communicate kindly and respectfully at all times. Students must not participate in harassing or bullying others online.
12. Students must comply with website terms of use, including age restrictions, appropriate access to the site, and use of resources.
13. Students should not forward chain letters, spam, or other unsolicited communications except to report these to ICT staff.
14. Students must not participate in business activities that are not staff-approved or done so as part of curriculum learning.
15. Students must not violate any state or federal laws, including the purchase of illegal items or substances, criminal activities punishable by law, etc.
16. Students must not take photos or videos of another individual without their consent.
17. Students should not use school or department ICT assets to stream or upload large volumes of data unless in the course of curriculum activities (e.g., streaming services such as Netflix, online gaming, livestreaming, etc.).
18. Students must not connect unapproved hardware to any school or department network.
19. Students must not install unapproved software on school or department-issued devices.
20. Security software approved by the school should be installed on all devices connected to the school network or other department networks.
21. All students must report suspicious activity or violations of this policy to a staff member.

Our school and the department reserve the right to monitor the use of ICT assets used by students. Students that misuse assets or use assets in an inappropriate manner may have their access revoked or be subject to other in-school consequences.

**To the parent/caregiver/legal guardian:**

Please read this page carefully to check that you understand your responsibilities under this agreement.

I understand that Kangaroo Inn Area School will:

* do its best to enhance learning through the safe use of ICTs. This includes working to restrict access to inappropriate, illegal, or harmful material on the Internet or on ICT equipment/devices at school, or at school-related activities.
* work with children and their families to encourage and develop an understanding of the importance of cyber-safety through education designed to complement and support the Use Agreement initiative. This includes providing children with strategies to keep themselves safe in a connected online world.
* respond to any breaches in an appropriate manner.
* welcome enquiries at any time from parents/caregivers/legal guardians or children about cyber-safety issues.

My responsibilities include:

* discussing the information about cyber-safety with my child and explaining why it is important.
* supporting the school’s cyber-safety program by emphasising to my child the need to follow the cyber-safety strategies.
* contacting the principal or nominee to discuss any questions I may have about cyber-safety and/or this Use Agreement.



**KIAS - Acceptable Use Acknowledgement**

**Students**

I have read and understood my obligations in relation to acceptable use of ICT assets at school. I understand that my access to the Internet and other computer resources may be revoked if I fail to comply with the policy, and acknowledge that my activities using ICT assets may be monitored by the school.

|  |  |
| --- | --- |
| **Student name:** |  |
| **Class/Homegroup:** |  |
| **Signature of student:** |  |
| **Date:** |  |

**Parents, Caregivers and Legal Guardians**

I have read and understood my child’s obligations in relation to acceptable use of ICT assets at school. I understand that my child’s access to the Internet and other computer resources may be revoked if they fail to comply with the policy. I have ensured that my child has signed this agreement, and discussed appropriate use and strategies to stay safe online with my child.

I understand that additional resources for parents on keeping children safe online is available on the eSafety Commissioner’s website, [eSafety.gov.au](https://www.esafety.gov.au/parents).

I consent to the use of Department endorsed technology products and services provided by the school for my child, including but not limited to Microsoft 365 and Google Workspace for Education and agree to the relevant terms and conditions of those products and services.

|  |  |  |
| --- | --- | --- |
| **Name(s):** |  |  |
| **Signature(s):** |  |  |
| **Date:** |  |  |

Please return this section to the school and keep a copy for your own reference.