

## East Para Primary School ICT and Cyber Safety User Agreement

Dear Parents/Caregivers,

Information and Communication Technologies (ICT) bring great benefits to the teaching and learning programs at East Para Primary School and to the effective operations of the school. We aim to maintain safe usage of all ICT's through the creation of a cyber-safe culture that is in keeping with our values and with legislative and professional obligations.

To assist us to enhance learning through the safe use of information and communication technologies (ICTs), we have attached a **User Agreement Form** to this letter to provide information and to seek consent and agreement for your child to use ICT's at school.

We ask that you read through and share with your child the information provided on the first two pages of this document. Once read and shared, please sign and return the third page to acknowledge that your child is fully aware of their responsibilities. Access to ICTs at school will then be ongoing unless responsibilities are breached.

### Strategies to help keep EAST PARA PRIMARY SCHOOL Students Cyber-safe.

**Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices regardless of the time of day.**

**Being cyber-safe is no exception and we invite parents/caregivers to discuss the following information and agreements with their children to help them stay safe when using ICTs at school and after formal school hours.**

1. ICT equipment is provided at school for learning experiences only.
2. Students may only access digital devices and the internet at school when teacher permission is granted and are present.
3. Students with queries regarding ICT use must ask a teacher prior to use.
4. Students must only log on with their own accounts and must not allow anyone else to use their school account. Passwords must be kept private.
5. The internet, email, digital devices or any ICT equipment and devices must be used 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 it intended "as a joke."
6. While at school, students will:
  - Only attempt to search for things online that they know are acceptable at our school and are linked to their learning. This would exclude anything that is rude or violent or uses unacceptable language
  - Report any attempt to bypass security, monitoring and filtering that is in place at our school.
7. If students find anything online that is upsetting, mean or rude, or is known to be unacceptable at our school, they will:
  - Not show other students
  - Turn off the screen
  - Seek teacher support

8. To ensure compliance with copyright laws and minimise corruption from viruses, the downloading or copying of files such as music, videos, games or programs can only be done with the permission of IT staff.
9. Teacher and/or parent/caregiver permission is required before any personal information is posted or shared online. Personal identifying information includes any of the following:
- Full name
  - Address
  - Email address
  - Phone numbers
  - Photos
  - Date of birth
  - School and class
10. All school equipment/devices must be treated 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
  - Following all school cyber-safety strategies, and not joining other students who choose to be irresponsible with ICTs
  - Reporting any breakages/damage to a staff member as soon as it happens.

11. If students do not follow cyber-safety practices the school may inform parents/caregivers.

In serious cases, **the school may take disciplinary action and families may be charged for repair costs. Repairs/replacements can range from \$600.** 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 personal items securely for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.

### **Information re Monitoring and Filtering at East Para Primary School**

Material sent out and received using school networks may be monitored and filtering software may be used to restrict access to certain sites and data, including email. Where a student is suspected of an electronic crime, this will be reported to the South Australian 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 Department for Education administrators to prevent children's exposure to inappropriate content when using the department's online service, it is not possible to completely eliminate the risk of such exposure. In particular, the Department for Education cannot filter internet content accessed by your child from home, from other locations away from school or on mobile devices using public Wi-Fi. The Department for Education recommends the use of appropriate internet filtering software.

This agreement will be periodically reviewed and updated as new technologies evolve, to ensure it is relevant, current and addressed identified issues.

ICT questions can be sent to the school's email address and will be forwarded to IT staff and Leadership to address and respond.

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.kidshelpline.com.au> and Bullying No Way at <http://www.bullyingnoway.com.au>.

## East Para Primary School ICT and Cyber Safety Agreement

Dear Parents/Caregivers,

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

### **I (parent/caregiver) understand that East Para Primary 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 User Agreement initiative. This includes providing children with strategies to keep themselves safe in a connected online world.
- Respond to any breaches or alerts from the Swift Portal in an appropriate manner. This may include prohibition of use of school devices for a period of time to be determined based on seriousness of breach.
- Welcome enquiries from parents/caregivers/legal guardians or children about cyber-safety issues.

### **My (parent/caregiver) 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 (listed on previous page)
- Contacting Leadership to discuss any questions I may have about cyber-safety and/or this User Agreement.

### ICT and Cyber-Safety User Agreement (Please return this page only to school)

We (parents/caregivers and student) have read and understand the ICT and Cyber-Safety User Agreement and are aware of the school's initiatives to maintain a cyber-safe learning environment.

Name of student \_\_\_\_\_ Class \_\_\_\_\_ Date \_\_\_\_\_

Name of parent/caregiver \_\_\_\_\_

Signature of parent/caregiver \_\_\_\_\_

Signature of student \_\_\_\_\_

**Please note: This agreement will remain in force as long as your child is enrolled at East Para Primary School. If it becomes necessary to add/amend any information or rule, you will be advised in writing.**