Tarlee Primary School

Acceptable use of Technology and Internet Policy

This policy is part of a series of inter related policies for the safety and wellbeing of students, parents, volunteers, visitors and any other person who come onto the school site.
This policy should be read in conjunction with the following other site policies:

- Cyber safety and Anti-Bullying Policy
- Mobile Phone Policy
- Anti Bullying Policy
- Behaviour Management policy
- Grievance Policy
- Student Wellbeing Policy

Acceptable Use of ICT Agreement:

The measures to ensure the cyber-safety at Tarlee Primary School outlined in this document are based on our schools core values.

The school's computer network, Internet access facilities, computers and other school ICT equipment/devices bring great benefits to the teaching and educational programmes and to the effective operation of the school.

Our school has rigorous cyber-safety practices in place, which include cyber-safety use agreements for all school staff and students.

The overall goal of the school in this matter is to create and maintain a cyber-safety culture which is in keeping with the values of the school, legislative and professional obligations. This use agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches which undermine the safety of the school environment.

Rationale:

Our students have access to Information and Communication Technologies at school including access to our school network of computers, the Internet, digital cameras and video, scanners, and interactive whiteboards. We consider that the use of these technologies has the potential to extend, enhance and transform student's learning, with particular relevance to an Inquiry methodology.

The goal of all ICT use at school is improved learning outcomes for our students. Appropriate use of the network, including the Internet, reflects high ideals of honesty, integrity, and consideration for others. It demonstrates respect for the intellectual property rights of others, for an individual's rights to privacy, as well as rights to freedom from intimidation, harassment and unwarranted annoyance

Internet Access and Duty of Care:

Access to the Internet at Tarlee Primary School is provided by DECS through a connection with sa.edu which provides support for the school to manage and monitor the appropriate use of the internet and minimise risks to students.

Tarlee Primary School staff are committed to educating students about the safe and responsible use of the Internet. Access to the Internet is viewed as a privilege. Users breaking the rules will not be permitted to use the school's facilities for a period of time.

While we are able to ensure a level of safety through filters which block inappropriate websites and monitoring of student use of our systems, there will always be the possibility that students may access inappropriate material via the Internet, use our network for time wasting or non-learning purposes, or use e-mail to communicate in an inappropriate manner. We consider the best policy is a mix of school controls and blocks, while teaching students to use ICT in a responsible and principled manner.

General Information:

The Tarlee Primary School Cyber Safety and Anti-Bullying Policy and Acceptable Use Policy applies to all persons employed, studying, or regularly attending the site. The use of all technology includes desktop computers, laptops, all mobile devices including cameras, the Internet, photocopiers, scanners and telecommunication systems used both on and off school grounds.

The school's computer network, Internet access facilities, computers and other school ICT equipment/devices are for educational purposes appropriate to the school environment. Staff may also use school ICT for professional development and personal use which is both reasonable and appropriate to the school environment. This applies whether the ICT equipment is owned or leased either partially or wholly by the school, and used on or off the school site.

The school reserves the right to confiscate and check the contents of electronic equipment where there is reasonable suspicion that the device contains material which contravenes Tarlee Primary School rules or the law; such as pornographic, violent or inappropriate images.

The use of Internet and online communication services can be audited and traced to the accounts of specific users. The school limits the size of email attachments (the current size limit is 2 Megabytes).

The Systems Administrator has responsibility for determining the extent to which software may legally be used.

Students, Parents and Volunteers: have access to curriculum computers only and have a designated folder in which to store their files. Students in years 3 and above have the opportunity to hire a portal storage device from the school to transfer their working files between home and school.

Staff: will have access to both the curriculum and administrative computer networks. Staff have designated folders for their work on both networks, but they are strongly encouraged to save their work on a personal, portable storage device. Staff may also have limited access to DECS applications through Edu Portal and EDSAS; after application for permitted access all of which are pass word protected.

Leadership and Administration: only have access to all Drives and any DECS applications through Edu Portal and EDSAS; after application for permitted access all of which are pass word protected.

All staff, students and volunteers: *whether or not* they make use of the school's computer network, Internet access facilities, computers and other ICT equipment/devices in the school environment, will be issued with a use agreement. Any staff member, volunteer or parent who has a signed use agreement with the school, and allows another person who does not have a signed use agreement to use the school's ICT equipment, is responsible for that use.

Responsibilities of Principal/System Administrator:

- Reviewing user statistics & filtering tools, blocking access to inappropriate sites where necessary.
- Filter specific words & phrases that could be used for inappropriate searches or messages.
- Monitor and update the network's anti-virus software.
- Manage & monitor user accounts, Internet history, Email use, and printing.
- Inform leadership of any instances of misuse of the Internet, Email service, or other ITC equipment.
- Should a child or teacher encounter unsuitable material through using the DECS Connect service, this will be reported to DECS CONECT helpdesk number as a matter of urgency by the site administrator.

Under regulations 40 and 41 of the Education Regulations 1997, principals can suspend or exclude a student who acts in a manner that threatens the safety or wellbeing of a student or member of staff, or another person associated with the school*. These regulations do not preclude an event that occurs outside of school hours or off site. Principals can therefore use these procedures with a student enrolled at their school if the principal believes, on reasonable grounds, that the student has acted in such a manner, even if this behaviour occurred outside of school hours or off site. Police officers also have the power to confiscate a mobile phone where any image held on the phone is possible evidence of a crime. The phone may be kept by SAPOL until the action comes before a court. Where DECS staff reasonably suspects that a student has used a mobile phone to record a crime, the phone should be confiscated and handed to SAPOL* ***without the staff member opening the video message to view it.*** *Opening the video message may compromise evidence. Providing this advice to your school community will support the implementation of the Keeping Safe Child Protection Curriculum which includes content on the safe use of new technologies*.

Responsibilities of Staff:

- Discuss the contents of this policy in detail before permitting students to use Internet facilities.
- Staff are expected to follow the instructions of the system Administrator regarding their role in maintaining cyber safety
- Ensure students understand their obligations, rights and responsibilities. Endeavouring to check that all students in their care understand the requirements of the student agreement.
- Regularly reminding students of the contents of the use agreement they have signed, and encouraging them to make positive use of ICT
- Develop student ICTs skills & knowledge; Teach students how to access and use the ITC equipment correctly and Staff should guide students in effective strategies for searching and using the Internet.
- Preview topic specific sites for students prior to commencing Internet use

- Provide adequate supervision for students whilst accessing Internet resources
- Provide and keep up to date a list of safe, appropriate and approved game sites for students to access.
- Observe copyright laws – Use the Internet as a source or a guide for information [*Copyright laws protect authors and publishers by giving them certain exclusive rights to their material. In addition, copyright laws provide an environment where the creative future of the nation is protected and promoted. Unauthorised copying deprives authors and publishers of valuable income and reduces the incentive to create new works. In all cases the user may only reprint, download, or copy information in accordance with the provisions of the Copyright Act. (See www.smartcopying.edu.au) Copyright laws also specifically protect software.]*
- If staff is aware that a student has not signed a use agreement, the student will not be permitted to use school ICT unless there are special circumstances approved by the principal.
- Staff must follow procedures relating to the school cyber safety incident book. Any incidents involving the unintentional or deliberate accessing of inappropriate material by staff or students must be recorded in handwriting in the cyber safety incident book with the date, time and other relevant details.
- Report the incident as soon as practicable to the system Administrator.
- Follow up on any known or suspected inappropriate use of any ICT hardware, software and Internet use.
- Inform leadership of any instances or suspected instances of misuse of the Internet, Email service, or other ITC equipment.
- Should a child or teacher encounter unsuitable material through using the DECS Connect service, Inform leadership as a matter of urgency by the site administrator.

Responsibilities of Students:

- Abide by all signed agreements for the use of ITC at Tarlee Primary School.
- Access school computers, the internet and printers using only their own user
- accounts. Keep passwords secret, and not allow others to use or access their accounts.
- Report to staff if others are using their accounts
- Use computers, software, the Internet, scanners digital cameras and video camera **only** for classroom or approved projects,
- Access the Internet only when given teacher permission. Internet games are not to be used unless part of a class school project.
- Will not download graphics, sound or video files, or software without the direct permission of a teacher, for use in a class project.
- Ask an adult before printing material especially from the Internet.
- Should they encounter inappropriate material on line they must:

IMMEDIATELY Turn off the screen.
Report immediately to the teacher or supervising adult who will record the URL and other details.

Refrain from describing or encouraging others from accessing the site either directly or through a search engine.
(Students may use the "Hector Safety Button" if available).

- Observe copyright laws – Use the Internet as a source or a guide for information
  [Copyright laws protect authors and publishers by giving them certain exclusive rights to their material. In addition, copyright laws provide an environment where the creative future of the nation is protected and promoted. Unauthorised copying deprives authors and publishers of valuable income and reduces the incentive to create new works. In all cases the user may only reprint, download, or copy information in accordance with the provisions of the Copyright Act. (See www.smartcopying.edu.au) Copyright laws also specifically protect software.]
- Log off at the end of each session to ensure that nobody else can use their
- account;
- Not damage or disable computers, computer systems or networks
- Not change or delete any application or file belonging to another person;
- Check email frequently, delete any unwanted messages promptly & stay within your email quota.
- Refrain from using e-mail or the internet in a way that harasses other students
- Be prepared to be accountable for actions and for the loss of privileges

Cyber Safety:

All USERS WILL:

- Follow the Tarlee Cyber Safety and Anti-Bullying policy
- Will report if they receive a message that is inappropriate or makes them feel uncomfortable; and must follow procedures relating to the school cyber safety policy.
- Any incidents involving the unintentional or deliberate accessing of inappropriate material by staff or student's, must be recorded in handwriting in the cyber safety incident book with the date, time and other relevant details.
- Seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student;
- Not attempt to disguise their identities or transmit information in a way that makes it appear that the information comes from someone other than themselves;
- Ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests;
- Respect the personal privacy of others and never attempt to access others' files and information.
- Never publish or disclose the email address of a staff member or student without that person's express permission

- Recognise that the Internet is a public place and always take care to ensure their safety;
- Be careful of statements that might offend people; including the use of offensive language in any document or communication.
- Not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others;
- Never send or publish:
  - a message that was sent to them in confidence;
  - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments;
  - material that threatens demeans bullies or harasses another person or makes excessive or unreasonable demands upon another person,
  - sexually explicit or sexually suggestive material or correspondence; false or defamatory information about a person or organisation;
  - anything that uses the name of the School or its Logo, motto, or any similar items on personal websites, without the permission of the Principal;
  - Video or other images of members of the School community without the permission of the people involved.

- Follow the schools policy for the use of personal Mobile Phone Use on school grounds.

Responsibilities of Parents/Guardians:

Parents will be aware of many issues of appropriate use and Internet safety which occur while students are using computers at home. Some of these issues include using internet chat rooms and instant messaging with unknown people, accessing inappropriate material from the World Wide Web, use of internet games or hot mail accounts in inappropriate ways, the creation of personal websites which give information about self or fellow students, thus putting self or others at risk.
We advise parents to closely monitor the use of the Internet at home and providing advice about how to ensure internet safety for children.

- Discuss the fact that there are websites which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information on the Internet.
- Remind children that people on line may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
- Be aware that children may be using the Internet in places other than in their own home or at school.
- Mobile Phones; be aware of the safety issues regarding mobile phones. Increasingly these now have Internet access.

- Encourage children to talk about how they use mobile phones.
- Remind children not to give mobile numbers to strangers and people they do not know very well.
- Talk about responsible use of text messaging.
- monitor Internet use.
- Keep the computer in a communal area of the home.
- Ask children how the computer works.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing.
- Check internet history log. This will tell you what websites your child is frequenting.
- Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner.
- Support the school and its policies for Appropriate Use of ITC, Cyber Safety and Anti Cyber Bullying.

Filtering system for the Home Computer: 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
Kids Helpline at http://www.kidshelp.com.au
Bullying No Way at http://www.bullyingnoway.com.au