A Proactive Approach

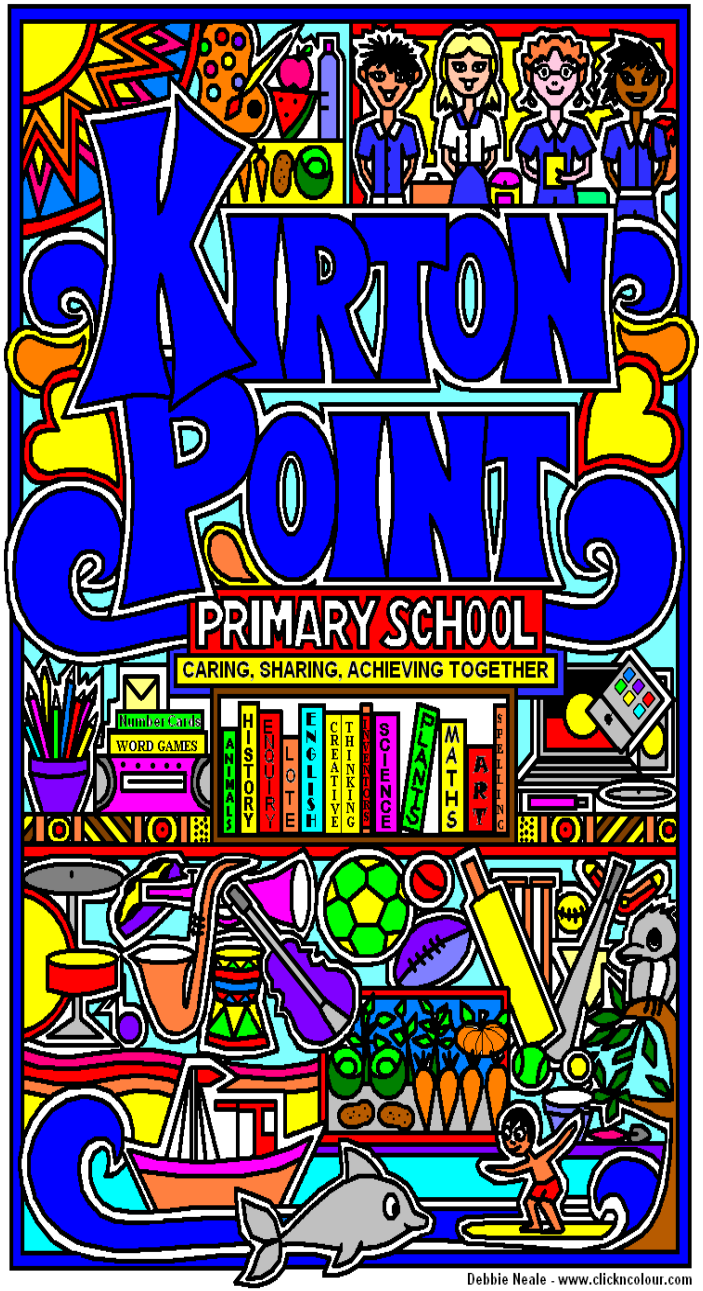
At Kirton Point Primary School, we do our best to ensure a cyber-safe learning environment by:

- Teaching all students the *Keeping Safe: Child Protection Curriculum,* which includes information and strategies around cyber-safety
- Monitoring and logging email traffic and Internet use, and providing filters to help guard against access to inappropriate materials
- Providing direction and advice about ICT (including the Internet & mobile phones) use and misuse, such as security & safety, bullying and e-crime
- Ensuring all students follow the copyright and licensing laws with respect to software, information and other material retrieved from or published on the internet
- Supporting police officers in undertaking an investigation and the collection of evidence following a report of suspected e-crime
- Following the cyber-safety guidelines outlined in the *Cyber Safety: Keeping Children Safe in a Connected World* document
- Making use of a range of cyber-safety resources to support teaching & learning
- Providing appropriate supervision for students when they are using ICTs

Caring, Sharing and Achieving Together

Matthew Place Port Lincoln SA 5606
P.O. Box 461 Port Lincoln SA 5606

Phone: 86821003
Fax: 86826266
E-mail: dl.0899_info@schools.sa.edu.au



Cyber-Safety Policy

Kirton Point Primary School Cyber-Safety Policy

Cyber-Safety

Our school is an exciting place to learn, especially with the opportunities our students have to take advantage of Information & Communication Technologies (ICT) to support and expand their learning. It is important however, to both protect and teach students while they learn to use ICTs and become responsible digital citizens.

Examples of ICTs at School

- Internet
- Computers, laptops, iPads
- Mobile phones
- Network software and hardware
- Web based tools and applications
- Interactive Whiteboards
- Storage devices (eg USB sticks)
- Digital cameras

ICT Expectations for Students

Students may only use ICTs for learning related activities that are approved by a teacher. They must not cause interference or disruption to other people or equipment, and may not access or distribute inappropriate material. This includes:

- Distributing spam messages or chain letters
- Accessing or distributing malicious, offensive, or harassing material, including jokes and images
- Bullying, harassing, defaming or giving offence to other people
- Spreading any form of malicious software
- Accessing files, information systems, communications, devices or resources without permission
- Using for personal financial gain
- Using non-approved file sharing technologies
- Using for non-educational related streaming audio or video
- Using for religious or political lobbying
- Downloading or sharing non-educational material

Students must also:

- Keep their log-in passwords confidential. They must not be written down or displayed anywhere, or shared with any other person
- Keep their personal or identifying information confidential at all times when using ICTs. This includes names, addresses, telephone numbers, images etc

Please Note:

- All students, staff and volunteers are expected to use ICT in a manner that ensures safety for the wellbeing of all others. Strict protocols apply to use of ICT. Misuse may result in restrictions or in severe cases, reporting the incident to the police.