



CYBER SAFETY

Policy

Purpose:

Fairhills PS has a responsibility to maintain a safe physical and emotional environment for all staff and students and recognises that the presence in the learning environment of technologies eg Internet, email, intranets, mobile phones short messaging service (SMS) and other ICT devices (some provided partly or wholly by the school and some privately owned by staff, students and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximise the benefits of these technologies, while at the same time to minimise and manage the risks. There is a need to have in place rigorous and effective school cyber safety practices which are directed and guided by an effective cyber safety policy.

General Aims:

- To ensure and reinforce the need for cyber safety for all students and staff within the school environment.
- To heighten awareness of both students and staff to the signs and evidence of cyber bullying and the need to report it whether as observer or victim.
- To ensure that all reported breaches of cyber safety are investigated appropriately and that support is given to both victims and perpetrators.
- To seek parental and peer-group support and co-operation at all times to ensure the safety and well-being of all students when using ICT technologies.

Implementation:

A. Primary Prevention

1. No individual may use the school Internet facilities and school-owned/leased ICT devices/equipment in any circumstances unless the appropriate use agreement has been signed and returned to the school. Use agreements also apply to the use of privately-owned/leased ICT devices/equipment on the school site, or at/for any school-related activity, regardless of its location. This includes off-site access to the school network from school or privately-owned/leased equipment.
2. The use agreements will cover all school employees, all students and any other individuals authorised to make use of the school Internet facilities and ICT devices/equipment, such as teacher trainees, external tutors and providers, contractors, and other special visitors to the school.
3. The use agreements are also an educative tool and should be used as a resource for the professional development of staff.
4. Use of the Internet and the ICT devices/equipment by staff, students and other approved users at Fairhills PS is to be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements.
5. Class teachers are responsible for establishing a system to ensure each student in their class has completed and signed a use agreement and that these forms are filed in a secure place.
6. The school has the right to monitor, access and review all use. This includes personal emails sent and received on the schools computer/s and/or network facilities at all times.
7. The school has the right to audit at anytime any material on equipment that is owned or leased by the school. The school may also request permission to audit

privately owned ICT devices/equipment used on the school site or at any school related activity.

8. Issues relating to confidentiality, such as sighting student or staff information, reasons for collecting data and the secure storage of personal details and information (including images) will be subject to the provisions of the Privacy Act.

B. Early Intervention

1. The safety of children is of paramount concern. Any apparent breach of cybersafety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the school's code of behaviour. In serious incidents, advice will be sought from the Conducts and Ethics branch of the DEECD
2. Students and staff will be encouraged to report bullying incidents involving themselves or others.
3. There will be regular monitoring on the school's computer networks to identify potential problems
4. Parents will be encouraged to contact the school if they become aware of a problem

C. Intervention

1. Once identified the bully, victim and witnesses will be spoken with, and all incidents or allegations of bullying will be fully investigated and documented.
2. Parents to be contacted.
3. Students identified by others as bullies will be informed of allegations.
4. Both bullies and victims will be offered counselling and support.
5. Removal of cyber-bullies from access to the school's network and computers for a period of time. Loss of privilege to bring a mobile phone to school for student's who bully via SMS or similar telephone functions.

D. Post Violation

- Consequences for students will be individually based and may involve:-
 - exclusion from class.
 - exclusion from yard.
 - school suspension.
 - withdrawal of privileges.
 - ongoing counselling from appropriate agency for both victim and bully.
- Reinforcement of positive behaviours.
- Support structures for both bullies and victims.
- Ongoing monitoring of identified bullies.

Resources:

- References: Safe Schools are Effective Schools booklet
www.curriculum.edu.au/mindmatters
- S428-2007 Cyber Bullying – Updating the Student Code of Conduct
www.bullyingnoway.com.au
<http://www.sofweb.vic.edu.au/wellbeing/safeschools/bullying/cyberbullying.htm#H3N400026>

Evaluation:

This policy will be evaluated in line with School Council cyclical review of policy documents and school and DEECD priorities.

This policy was last ratified by School Council in....

AUGUST 2008