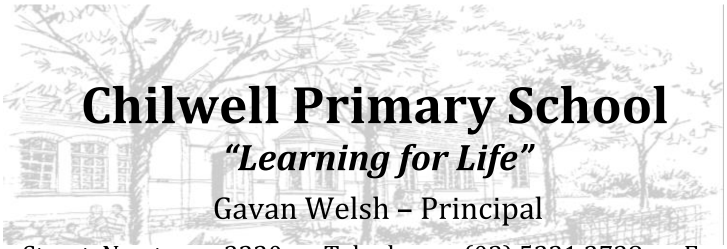

Chilwell Primary School

"Learning for Life"

Gavan Welsh – Principal

No.2061

313a Pakington Street, Newtown, 3220 Telephone: (03) 5221 2738 Fax: (03) 5221 8191
email: chilwell.ps@edumail.vic.gov.au ABN 43 418 945 496

POLICY: CYBERSMART

1. Rationale

Chilwell Primary School embraces the presence and use of Information and Communication Technologies (ICT) as an integral part of the learning environment. However, the use of ICT must be complemented by clearly articulated roles, responsibilities and expectations of those who use the technology. The CyberSmart policy seeks to ensure the safe and responsible use of ICT within the Chilwell school community,

Definitions

Cybersafety - the way in which users behave responsibly online to keep themselves and their friends safe. It incorporates the safe and desirable use of the internet and ICT equipment and devices, an awareness of our digital footprint, and how to behave appropriately and respectfully.

Cyberbullying – direct verbal or indirect bullying behaviours using digital technologies. This includes harassment via a mobile phone, setting up a defamatory website or deliberately excluding someone from social networking spaces.
(Sourced from www.education.vic.gov.au/school/principals/spag/safety/Pages/bullying.aspx)

2. Aims

- To promote the appropriate use of ICT by all members of the school community that ensures the safety and well-being of all students, staff and parents, emphasising a zero tolerance to cyberbullying.

- To ensure students, staff and parents are aware of their roles and shared responsibilities in relation to cyber safety and appropriate online behaviours.

- To develop the skills, knowledge, attitudes and behaviours required of students, staff and parents to participate and function responsibly, safely and appropriately in cyberspace.

3. Implementation

Chilwell Primary School promotes partnership between all members of the school community in adhering to this policy. Our approach to cybersafety aligns with our school values and is supported by our eSmart accreditation, *ICT Acceptable Use Agreement, the* '*You Can Do It*' program, the Student Engagement and Well-Being Policy, and our Privacy Policy.

4. Prevention

- The school is responsible for sourcing and implementing relevant and developmentally appropriate programs and strategies that promote positive online behaviours and cybersafe practices. A range of classroom-based, interactive, online student learning, staff professional learning, and parent education opportunities will be utilised such as eSmart initiatives, Connect Ed Online Program, Cybersafety experts, promoting cybersafe websites, support materials and publishing relevant information via school newsletter and Skoolbag App.
- All staff, students and parents are responsible for acting in accordance with the school's annual ICT User Agreements, and to work in partnership to ensure the safe and productive use of ICT.

- The school has the authority to monitor, access and review all school-based ICT usage by students, staff and parents. This includes emails sent and received on the school's computers and/or network facilities. The school has the authority to audit, at any time, any material located on equipment that is owned or leased by the school, or the school's network.
- Chilwell Primary School's Privacy Policy will support this policy.

5. Intervention

- Students, staff and parents will be advised to report any breaches of the ICT User Agreements or incidents of cyberbullying activity to a staff member, or through the Bullying Incident Notice (BIN) accessible via the school's intranet.
- Any incidences or allegations of behaviour that are in apparent breach of Chilwell's ICT User Agreements will be thoroughly investigated by the school.
- Significant breaches made by, or involving, students will result in the school immediately notifying the parents of those students.
- Where a breach is deemed to be extremely serious, DEECD's Conduct and Ethics branch may be contacted.
- The school's response to alleged breaches will involve dialogue with the person(s) who have allegedly committed the breach, and any person(s) harmed as a result of the alleged breach. This dialogue may result in subsequent action and/or user agreement privileges being reviewed. All actions and responses taken and proposed will be documented, and all persons involved will be informed. The school's response will also consider the ICT Breaches and Consequences drafted by Year 6 ICT leaders (currently being developed).
- The progress and well-being of any student involved in breaches will be monitored and evaluated in line with our Student Engagement & Well-Being Policy.
- Where cyberbullying has been identified, counselling and support may be offered, as determined by the school.
- Consequences of inappropriate use will follow the steps outlined in the Student Engagement and Welfare Policy, and the Year 6 ICT leaders Offences and Consequences document (under development).

6. Review

Due to the rapid evolution of ICT, regular evaluation and updating of this policy will occur when required, or annually at a minimum.

This policy was ratified by School Council on [#] August 2014 Review: Annually

Reference: DEECD – http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/princyber.aspx

Supporting documents:
- Acceptable Use Agreement
- Student Engagement and Welfare Policy
- Privacy Policy
- You Can Do It framework
- ICT Offences and Consequences (currently being developed by Year 6 ICT leaders)

Useful websites:
eSmart: http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/esmart.aspx
Acma: http://www.cybersmart.gov.au/parents.aspx
Help button: http://www.communications.gov.au/online_safety_and_security/cybersafetyhelpbutton_download

Policy Adapted and modified with permission from Hartwell Primary School's Cybersafety Policy