Cyber-Safety Policy

Cyber-Safety Policy

Measures to ensure the Cyber safety of Big Hill Primary School are based on our school values

- ***Be Respectful***
- ***Be Responsible***
- ***Be Safe.***

To assist us to enhance learning through the safe use of information and communication technologies (ICTs), all parents/caregivers are asked to read this document and sign a Use Agreement Form at the start of each year.

At Big Hill Primary School, we invest in network systems to manage and protect the welfare of children. However, the progression of wireless and mobile devices can allow children to bypass conventional network systems. This has the potential to expose young people to risks previously managed by filtered departmental and local systems. While we will continue to protect children's identity and learning examples we need to instil confidence in them to keep themselves safe and inform the adults around them if or when they feel uncomfortable, threatened or bullied - even if that occurs away from their school environment. The computer network, Internet access facilities, computers and other ICT devices bring great benefits to the teaching and learning programs at Big Hill Primary School, and to the effective operation of the school. The ICT equipment is for educational purposes appropriate to this environment, whether it is owned or leased either partially or wholly by the school, and used on or off the site.

The overall goal of Big Hill Primary School is to create and maintain a Cyber safety culture that is in keeping with school values and with legislative and professional obligations. The Use Agreement includes information about individual obligations, responsibilities, and the nature of possible consequences associated with Cyber safety breaches that undermine the safety of the school environment.

All students will be issued with a Use Agreement at the start of each year and once signed consent has been returned to school, students will be able to use the school ICT equipment.

Rationale:

Our school provides the students with ICT devices, Internet facilities and equipment to enhance and enrich learning outcomes and for the effective operation of the school. Big Hill PS recognises that whilst ICT provides significant educational value, it can pose a risk of exposure to inappropriate and offensive material and personal safety of students. It can facilitate anti-social, inappropriate and even illegal material and activities. Our school has the responsibility to maximize the benefits of these technologies, whilst at the same time minimising and managing the associated risks.

Big Hill PS acknowledges the need to have in place rigorous and effective cyber-safety practices, which are directed and guided by this cyber-safety and the Student Code of Conduct for Internet and Digital Technologies.

Definitions:

ICT (Information and Communication Technology) – means all the computer hardware, software systems and technology including internet, social network sites, telecommunication devices (mobile phones), web 2.0 tools, in facilities that may be used or access from the school campus or connected to a school's communication network.

Cyber-Safety – means the safe use of the Internet and ICT equipment/devices, including mobile phones.

Cyber-bullying – means bullying which uses technology as a means of victimizing others. It is the use of an Internet service or mobile technology (such as email, chat rooms, instant messaging, web pages, SMS, gaming sites) the intention of harming another person.

Inappropriate material – means material that deals with matters such as sex, cruelty, discrimination or violence in such a manner that is likely to risk student safety physically or emotionally, or is incompatible with the school environment.

E-crime occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

Technologies related to cyber-safety:
The current and emerging technologies used in school and more importantly in many cases, used outside of school by children include (but is not limited to):

- The Internet
- Emails
- Instant Messaging (Messenger, Facetime etc) which often use web cams
- Blogs
- Podcasts
- Social network sites (Facebook, Instagram etc.)
- Video broadcast sites (YouTube etc.)
- Chat rooms
- Gaming sites
- Music download sites
- Mobile phones, including those with camera and video functionality
- Smart phones with web functionality.

Big Hill PS documents to support a cyber-safe environment:

- Student Code of Conduct for Internet and Digital Technologies
- A Published Photos permission form
- Big Hill Facebook and Social Media policy
- SWPBS Matrix
- A PG viewing permission form

School Responsibility:
Material sent and received using the network may be monitored and filtered and/or monitoring software may be used to restrict access to certain sites and data, including e-mail. If illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform the Victorian 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. If students do not follow Cyber safety practices, the school may inform parents/caregivers, and in serious cases, may take disciplinary action against the student(s). Families may also be charged for any damage or repair costs where applicable.

While every reasonable effort is made by schools and DEECD administrators to prevent exposure of children to inappropriate content when using departmental online services, it is not possible to completely eliminate the risk of such exposure. In particular, DEECD cannot filter Internet content accessed by a child from home, from other locations away from school or on mobile devices owned by a child. DECD recommends the use of appropriate Internet filtering software on all devices.

Big Hill PS will take all reasonable steps and procedures to protect students from Cyber-bullying by:

- Incorporating Cyber Safety in the School Wide Positive Behaviour Program
- Incorporating Cyber-safety education into the curriculum taught.
- Using a filtered Internet service, which is designed to filter out inappropriate material.
- classes in "netiquette" in order to develop acceptable behaviours when online;
- That any breaches of this code (see signed permission form) will result in; investigation and possible withdrawal of privileges.

Note: No filtering service is 100% effective; therefore all student use of the Internet is supervised by an adult.

- Have policies and procedures in place regarding Internet use.
- If deemed necessary, inform DEECD of cyber-bullying incidents through appropriate channels.
- Consider informing the Police of cyberbullying incidents depending on the severity or repetitious nature of an offence.
- Ensures that information published on the Internet by students or the school is of a high standard, and meets legal requirements and standards of general practice within the community in relation to copyright, safety and decency.

Teacher's Responsibility:

The teachers of Big Hill PS will supervise and monitor all Internet use by students in their class. If a teacher is made aware of a cyberbullying incident he/she will do 1 or more of the following:

- Ensure the Student Code of Conduct is explicitly explained to all students.
- Gather as many facts about the case as possible.
- Discuss the incidents with all relevant parties.
- Advise the child not to respond to messages
- Secure and preserve any evidence.
- Consult the ICT Coordinator
- Refer to relevant policies and DEECD information (See reference links)
- Notify parents of children involved
- Report to a Principal class staff member.

Student's Online Responsibility:

Students at Big Hill PS will be expected to follow Cyber safe practices which aim to maximize the benefits of Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimizing and managing risks associated with internet use. These cyber-safe practices will aim to provide a Cyber safe school environment while addressing the needs of students to receive education about the safe and responsible use of present, and developing technologies.

Students will:

- Only use their own login username and password to access computers and other technological equipment, in the Middle and Senior Homesteads.

- Only use their class login username and password to access computers and other technological equipment, in the First Steps and Junior Units.
- Not change, delete or adapt other people's file/documents.
- Ask for permission before entering a website, unless a teacher has already approved this site.
- Never post fill names, addresses, phone numbers or any other personal details.
- Never provide full names, addresses, phone numbers or any other personal information of anyone else.
- Only send or post information or comments with teacher approval. Everything posted/sent must be checked by a teacher first.
- Tell a teacher if they have received a message they are not comfortable with or know of someone else receiving something hurtful.
- Not send/post photos or videos without checking with a teacher and having permission from parents.
- Not post photos of anyone in school uniform without permission
- Respect others and refrain from posting or sending messages that deliberately hurt, harass or threaten others.
- Keep and save any bullying emails, messages or images and show then to a teacher.
- Not reply to abusive or hurtful messages
- Act responsibly if inappropriate material has accidently been encountered by:
    - *Minimizing or quitting the tab*
    - *Reporting immediately to the teacher or supervising adult who will record the URL and other details*
    - *Refrain from describing and encourage others* to access the site.

Parent Information:

The school cannot be held responsible for student actions outside of the school premises. It is important for parents to promote cyber-safety in the home and monitor its use. Tips for parent to promote Internet safety in the home include:

- Discuss the Student Code of Conduct with your child
- Remind children to never give out personal information on the internet
- Be vigilant and monitor their time online. Be aware of excessive hours spent on the Internet
- Keep computers in a communal area of the home.
- Take an interest in what children are doing online.
- Check Internet history log. This will tell you what websites your child is frequenting.
- Have filter software installed on home computers.
- Discuss with your child how to response to unsuitable material or messages.
- See links below for tips and parent information.
- Be aware of age restrictions on social media websites e.g.: Facebook, Instagram etc.

Cyber-safety –Useful Websites:

Our school's cyber-safety practices are based on information contained in the latest version of the website, https://www.esafety.gov.au/ which is endorsed by the Victorian DEECD.

For more information on Cyber-Bullying and Cyber-Safety awareness, including tips on how to stay cyber-safe, the following links are recommended:

www.kidshelp.com.au

www.bullyingnoway.com.au
www.acma.gov.au
https://www.esafety.gov.au/

REVIEW CYCLE

This policy was last ratified by School Council September 2017 and is scheduled for review in September 2019