Policy No 87  

Cyber Safety

Written by: Lindy Powell and Cyber Safety Professional Learning Team

Date approved by School Council:

PURPOSE:

Chelsea Heights Primary School has a responsibility to maintain a safe physical and emotional environment for all staff and students. The school recognises that Information and Communication Technology is an integral component of Teaching and Learning. The school acknowledges the presence in the learning environment of technologies eg. Internet, email, intranet, 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), and acknowledges that these technologies can facilitate antisocial, inappropriate and even illegal material and activities. The school has a responsibility to maximise the benefits of these technologies whilst managing the risks by teaching safe use of ICT and awareness of the consequences of cyber bullying and harassment. A cyber safety policy will direct and guide cyber safety practices.

Cyber bullying is commonly defined as the use of information and communication technologies to support repeated and deliberate hostile behaviour intended to harm others. It is sometimes used as an extension to other forms of bullying, and can result in the target of bullying experiencing social, psychological and academic difficulties.

Children and young people can also be affected by hostile behaviour that does not fit the definition of cyber bullying. For example, a one off insensitive or negative remark or joke online or via text is not cyber bullying by definition. However, the impact can be widespread due to the rapid dissemination and the relative permanency of the message sent. For the purposes of brevity, both cyber bullying and other hostile cyber behaviours will be referred to as cyber bullying... for the purpose of this policy

- www.cybersmart.gov.au

AIM

- To educate the Chelsea Heights Primary School community about ICT and how to stay safe
- To ensure and reinforce the need for cyber safety for all staff and students within the school environment.
- To heighten awareness of staff and students to the signs and evidence of cyber bullying and the need to report it, whether as an 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 cooperation at all times to ensure the safety and wellbeing of all students at Chelsea Heights PS when using ICT.
IMPLEMENTATION

The staff of Chelsea Heights Primary School have the responsibility to ensure that:

- all forms of cyber bullying are prohibited at Chelsea Heights Primary School
- staff are aware of cyber bullying and are able to identify and look for signs of occurrence among the students
- students are aware of the consequences of cyber bullying
- a code of conduct is in use for technology, including computers and mobile phones, whilst on the school premises
- all cases of cyber bullying are reported to an Assistant Principal and responded to promptly
- there is supervision of technology that is effective for monitoring and deterring cyber bullying

The students of Chelsea Heights Primary School have the responsibility to ensure that:

- do not participate in cyber bullying
- do not use mobile phones, cameras or other digital devices to record audio and visual material that is not authorised as part of the school curriculum program
- do not breach the privacy of students, staff and members of the school community through any unauthorised recording or filming
- do not disseminate inappropriate information through digital media or other means
- report incidents of cyber bullying to a member of staff
- advise students being victimised by cyber bullying to talk to an adult
- offer to speak to an adult on behalf of the student who is being victimised by cyber bullying

REQUIREMENTS REGARDING APPROPRIATE USE OF ICT IN THE SCHOOL LEARNING ENVIRONMENT

In order to meet the school's legislative obligation to maintain a safe physical and emotional learning environment, and be consistent with the values of the school:

- The use of Chelsea Heights Primary School’s computer network, Internet access facilities, computers and other ICT equipment/devices is limited to educational and creative purposes appropriate to the school environment.

- Chelsea Heights PS has the right to monitor, access, and review all the use detailed above. This includes personal emails sent and received on the school’s computers and/or network facilities, either during or outside school hours if a need arises.

- The use of privately-owned ICT equipment/devices on the school site, or at any school-related activity must be appropriate to the school environment. Equipment/devices could include a mobile phone, camera, recording device, or portable storage (like a USB or flash memory device). Anyone unsure about whether or not it is appropriate to have a particular device at school or at a school-related activity, or unsure about whether the planned use of a particular device is appropriate, should check with the teacher and/or Principal.

Note that examples of a ‘school-related activity’ include, but are not limited to, an excursion, camp, sporting or school community event, wherever its location.
• The school takes all reasonable precautions to screen material being accessed through information systems such as the Internet. However, it may not always be possible for the school to filter or screen all material. This may include material which is inappropriate in the school environment.

_It is the expectation that each individual will make responsible use of such systems._

**MONITORING BY THE SCHOOL**

• The school monitors traffic and material sent and received using the school’s ICT infrastructures. This may be examined and analysed to help maintain a cyber safe school environment when the need arises.

• The school will deploy filtering and/or monitoring software where appropriate to restrict access to certain sites deemed appropriate by the principal and teaching staff with the support of the computer technicians

_However, the expectation is that each individual will be responsible in their use of ICT equipment._

• Users must not attempt to circumvent monitoring or filtering

**AUDITS**

• The school will regularly conduct an internal audit of its computer network, Internet access facilities, computers and other school ICT equipment/devices,

• Where deemed necessary, stored content will be deleted. Staff and students will be notified prior to this taking place.

**BREACHES OF AGREEMENT**

• Breaches of the use agreement can undermine the values of the school and the safety of the learning environment, especially when ICT is used to facilitate misconduct. Such a breach, which is deemed harmful to the safety of the school (for example, involvement with inappropriate material, or anti-social activities like harassment), may constitute a significant breach of discipline and result in serious consequences. The school will respond to any breach of the use agreement in an appropriate manner, taking into account all relevant factors on a case by case situation. Depending on the seriousness of a particular breach, possible school responses could include one or more of the following: a discussion with the student, informing parents, loss of ICT privileges, the family having responsibility for the cost of ICT repairs or replacement, the school taking disciplinary action which is outlined within the schools behaviour management policy.

• If there is a suspected breach of use agreement involving privately-owned ICT e.g. (USB flash drive) on the school site or at a school related activity, the matter may be investigated by the school. The school may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.

• Involvement with material which is deemed inappropriate in a school setting, is a very serious matter, as is involvement in an activity which might constitute criminal misconduct, such as cyber bullying. In such situations parents will be contacted and it may be necessary to involve law enforcement in addition to any disciplinary response made by the school.
OTHER ASPECTS OF THE SCHOOL’S CYBER SAFETY PROGRAMME

The use agreements operate in conjunction with other cyber safety initiatives, such as cyber safety education supplied to the school community. This education plays a significant role in the school’s overall cyber safety program, helping students to be cyber safe in all areas of their lives.
CYBERSAFETY RULES FOR STUDENTS
SECTION 1

**Note for Parents/Legal Guardians/Caregivers:** The sections marked **are designed to provide a guide to the rules covered by this use agreement, and to help you discuss the rules with your child. Teachers will also outline to students their responsibilities when using the schools ICT equipment and network. The meaning of ‘ICT’ or ‘ICT equipment/devices’ can be found on page one.

1. I must have a use agreement signed by me and by my parent or caregiver before I am allowed to use the school ICT equipment.

   **All students, regardless of age or ability, must have a use agreement signed by their parent. All students sign their use agreements along with their parents. Use agreements are becoming accepted as an essential part of cybersafety policy and programmes for schools and other organisations, including businesses.**

2. I can use the school computers and other school ICT for uses the school deems appropriate.

   **This helps to ensure the equipment is available when students need to use it for their learning. It will also help to reduce the likelihood of any inappropriate activities taking place which put at risk the safety of the learning environment.**

3. If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.

   **This helps the students of Chelsea Heights PS to take responsibility for their own actions, and seek advice when they are unsure of what to do. It provides an opportunity for the teacher and student to work through an issue and so avoid the student making an unwise decision which could possibly lead to serious consequences. Young children need ongoing advice and guidance to help them become safe and responsible users of ICT.**

4. I will follow the cybersafety rules, and will not join in if others are being irresponsible. I will tell the teacher of such behaviours straight away.

   **Unfortunately, along with many benefits, technology has also provided new ways to carry out anti-social activities. Bullying and harassment by text message, for example, is becoming a major problem in Australia and in many other countries. Often children become involved in these acts through peer pressure, without thinking of the consequences.**

5. If I accidentally come across mean, rude, or dangerous material I will tell the teacher straight away, without showing any other students. The teacher will then notify the network administrator to block this material.

   **Because anyone at all can publish material on the Internet, it does contain material which is inappropriate, and in some cases illegal. The school takes a number of steps to prevent this material from being accessed. However, there always remains the possibility that a student may inadvertently stumble across something inappropriate. Encouraging students to tell a teacher immediately if they find something which they suspect may be inappropriate, encourages critical thinking and helps students to take responsibility for their actions and keep themselves, and others, safe. This way, they contribute to the cybersafety of the school community.**

6. If I am not feeling safe at any time while using the ICT equipment, I will tell the teacher straight away.

   Chelsea Heights PS strives to create a safe and secure learning environment for all members of the school community. Examples of situations involving the use of ICT which might cause a student to feel unsafe could include: contact being made by a stranger through email or text message, the presence of ‘scary’ images on a computer screen, and/or misconduct by other students. Staff need to be made aware of such situations as soon as they occur to ensure the school can respond immediately.
7. I will only log onto the school network using my user account/class room number.

8. I will not share my password with any other person.
**Passwords perform two main functions. Firstly, they help to ensure only approved persons can access the school ICT facilities. Secondly, they are used to track how those facilities are used. Knowing how the equipment is being used and by whom, helps the school to maintain a cybersafe environment for all users, and teaches the student the importance of personal security.**

9. I will log off or shut down the computer when I have finished using it.

10. I will log off before letting someone else use the computer.
**Logging off or shutting down, stops others from using a computer under your child’s username. When the computer is started up again, the next user has to enter their own details to log on.**

11. If I am sharing a computer which is logged on under my name/by me, I am responsible for how it is used. If there is a problem, I will tell the teacher immediately.
**Students often work together at a single computer. It is important that your child takes responsibility for sensible use of the computer at all times, and tells the teacher if there is any concern.**

12. I will check with the teacher/parent before giving anyone information about myself or others when using the Internet – this includes name, home and email addresses, and phone numbers.
**This reduces the risk of students being contacted by someone who wishes to upset or harm them, or use their identity for purposes which might compromise the student’s privacy or security online.**

13. I will not be careless, try to damage, or steal any school ICT equipment. (If this happens, the school will need to inform my parents about what has happened. My parents may have responsibility for the cost of repairs or replacement.)

14. I will not try to stop the network or any other equipment from working properly.

15. If I accidentally break school ICT equipment, damage it through mishandling, or I find it broken when I start to use it, I will tell a teacher straight away.

16. I will not change any screensavers, desktop backgrounds, themes or hardware settings.

17. I will have no involvement with making or sending malware (such as viruses, worms & trojans) on purpose.

18. I will use good judgement to decide whether printing is necessary. If I am unsure I will seek advice from a teacher.
**Rules 12-18 are designed to help protect the investment the school has made in expensive ICT technologies. Also, certain settings may have been applied to maximise the safety of the students and the equipment (such as antivirus settings or restrictions on Internet access).**

19. I will not download any files such as music, videos, or programs.
Many files available on the Internet are covered by copyright, and although they can be easily downloaded, it may be illegal to do so. Sometimes even innocent-looking files may contain malicious content such as viruses,
or spyware (software that searches for personal information from your computer and transmits it to others over the Internet). As well, some files may contain inappropriate or illegal material.

20. I must have permission from school, before bringing any disk or other ICT equipment / device from home. If I am given permission, then I must use that ICT sensibly.

** The devices referred to in this rule include those specified on page one of this document; for example flash memory devices, iPods, MP3 players or mobile phones. Any students bringing such devices from home are asked to use them sensibly. This applies to the school site, and any school-related activity. This rule is designed to protect the school’s online security and equipment from viruses which can easily be transferred using disks or other storage devices such as memory cards. NB Parents should be mindful of the school’s specific policy regarding students and mobile phones. You might like to take this opportunity to have a discussion with your child about their general use of ICT whether in or out of school. It helps keep children cybersafe if they understand that many of these rules should be followed regardless of whose ICT equipment they are using, where they are (for example at home, at school, or at a friend’s house), or who they are with.

21. I will not bring software or games from outside school to use on school equipment.

** Installing software from home may cause conflicts with the software installed by the school. Chelsea Heights Primary School must also abide by any licensing requirements included within the software. This means that unless the school has purchased a copy, it will not usually be legally entitled to install the software. And as mentioned in point 19, inappropriate or illegal content may be involved.

22. I will acknowledge where work has come from if I have copied it from somewhere. This includes graphics and sounds files I use in my own schoolwork.

** The Internet has allowed easy access to a huge range of information which can be incorporated into students’ work by simply cutting and pasting. Most of this material is copyrighted, and thus involves intellectual property issues. Also, the value to students’ learning is questionable if they have not thought through this information themselves.

23. I will check with the teacher before using school equipment to copy software, music, videos or other files, in case they are copyrighted.

** Any such copying is likely to be restricted by copyright laws. Chelsea Heights Primary School will not condone the use of its equipment for these activities.

24. I will not use the internet, mobile phones or any other ICT equipment to be mean, rude, offensive, or to harass any members of the school community like students and staff, while at school or when involved in any school-related activity. The same rule applies when using school ICT at any time, whether at school or not.

** The basic principles of respect extend to the use of information and communication technologies. The capacity of ICT to increase the scale and scope of misconduct can make an otherwise minor rule infringement into a much more serious matter. For example, name calling often becomes a more serious issue where texting or emailing has been used to facilitate harassment. Cyber bullying can involve a range of misconduct including the creation of abusive websites.

25. If I break these rules, the school may need to talk to my parents about what has happened. Disciplinary action should be expected.

Depending on the seriousness of a particular breach, possible school responses could include one or more of the following: a discussion with the student, informing parents, loss of ICT privileges, the parents possibly having responsibility for the cost of ICT repairs or replacement, the school taking disciplinary action.
TO THE STUDENT AND PARENT/LEGAL GUARDIAN/CAREGIVER:

Please read this page carefully as it includes information about your responsibilities under this agreement.

- Complete and sign the appropriate section.
- Detach and return Section 2 to the school.
- Keep Section 1 for your future reference.

CHELSEA HEIGHTS PRIMARY SCHOOL WILL:

- do its best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or school ICT equipment/devices at school or at school-related activities
- work with children and their families to encourage and develop an understanding of the importance of cyber safety through education designed to complement and support the use agreement initiative. This includes providing children with strategies to help keep themselves safe in cyberspace
- keep a copy of this signed use agreement form on file
- respond to any breaches in an appropriate manner
- welcome enquiries from parents or students about cyber safety issues.

SECTION 2

Student’s section

MY RESPONSIBILITIES INCLUDE:

- I will read this Cyber safety Use Agreement document carefully with my parent or caregiver
- I will follow the cyber safety rules and instructions whenever I use school ICT
I will also follow the cyber safety rules and instructions whenever I am involved with privately-owned ICT on the school site or at any school-related activity.

I will have no involvement in use of ICT which could put me at risk, or other members of the school community.

I will take proper care when using computers and other school ICT equipment/devices. If I have been involved in the damage, loss or theft of ICT equipment/devices, my parents may have responsibility for the cost of repairs or replacement.

I will ask my teacher or my parents if I am not sure about something to do with this agreement.

I have read and understand my responsibilities, and agree to follow the Cyber safety Use Agreement.

I know that if I breach this use agreement, there may be serious consequences.

Name of student: _____________________________

Class: ____

Signature: _______________________________

Date: ____________

Section for parent/legal guardian/caregiver

MY RESPONSIBILITIES INCLUDE:

- I will read this School Cyber safety Use Agreement document and discuss the rules with my child.
- I will ensure this use agreement is signed by my child and by me, and returned to the school.
- I will support the school's cyber safety program by encouraging my child to follow the cyber safety rules, and to always ask the teacher if they are unsure about any use of ICT.
- I will contact the School to discuss any aspect of this use agreement which I might want to learn more about.
- I will take every precaution to ensure that any file transferred to the school is virus free.
I have read this Cyber safety Use Agreement and am aware of the school’s initiatives to maintain a cyber safe learning environment, including the responsibilities involved.

Name: ____________________________________________

Parent/Legal Guardian/Caregiver (please circle which term is applicable)

Signature: ___________________________ Date: __________