Pearcedale Primary School

Together Everyone Achieves More

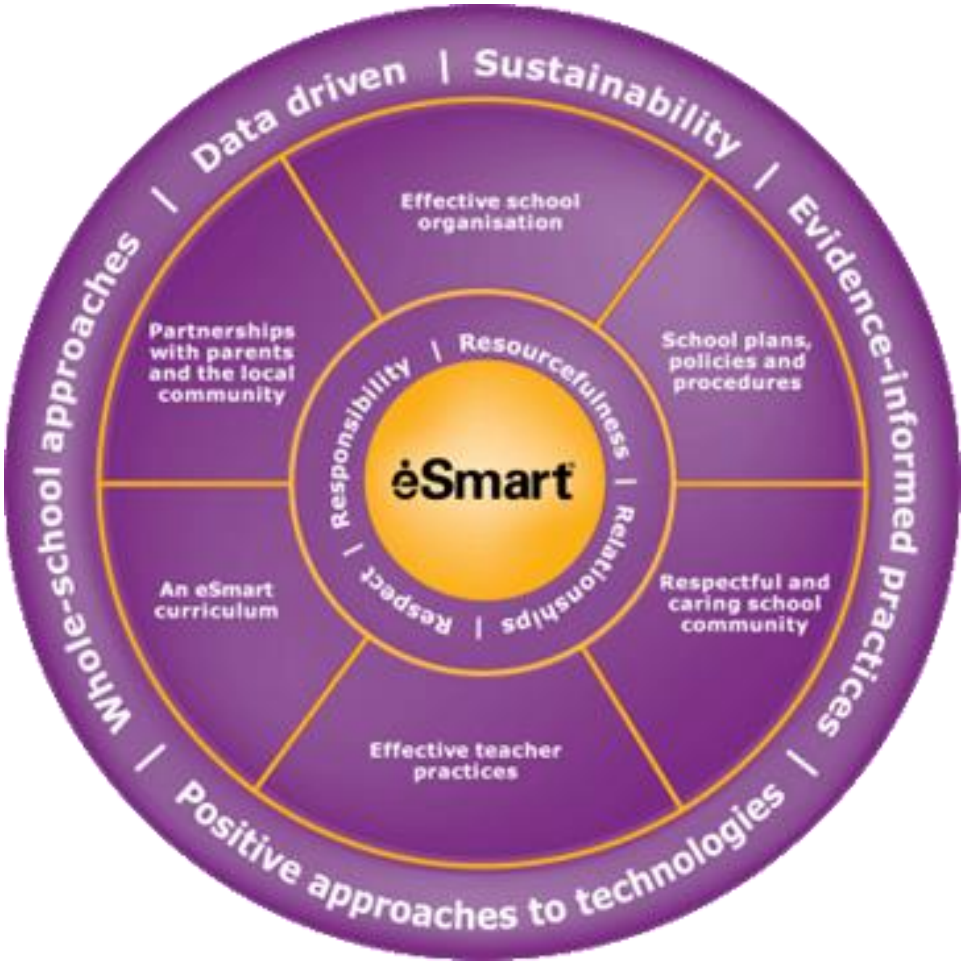
E-Smart Student Welfare Policy

eSmart®

What is E-Smart?

This whole-school cybersafety and wellbeing framework assists students, teachers and the wider school community to embrace the best that new communication technologies and media can offer, while being savvy about the risks.

Being eSmart means knowing how to guard against the security and privacy risks online, being able to research and reference information and download content in ways that are ethical and legal, as well as being able to manage reputation and relationship-based issues associated with being in cyberspace.



CONTENTS

1.0- Rationale

Pearcedale Primary School has a commitment to providing an educational environment that is safe and supportive. Within this, we acknowledge that technology is becoming an increasingly integral part of everyday life and we place a high priority on providing Internet facilities and ICT devices/equipment which will benefit student learning outcomes and the effective operation of our school. We also recognise that the presence in the learning environment of these technologies (whether provided by the school or privately owned by the staff, students and other members of our community), can also facilitate anti-social, inappropriate and even illegal, materials and activities.

Our school, therefore, has the dual responsibility to maximise the benefits of these technologies, while at the same time to minimise and manage the risks. With this is mind, the 'Pearcedale Primary E-Smart Student Welfare Policy' has been developed to encompass existing and new technologies and their effects on the lives of the school community. Not only does this policy affect what happens within the school, it also promotes the safety and wellbeing of the students when they are not in direct care. Through increased awareness, we aim to facilitate the development of a community and environment that is not only 'cyber savvy' but cyber safe.

We at Pearcedale Primary believe that every child has the right to leave with the skills required to participate fully in an increasingly technological society. We want our students to become confident, skilled and critical in their use of technologies and to be able to interpret information from a variety of sources. The Internet provides a powerful resource for learning as well as an efficient means of communication. As we educate our students for a rapidly changing world we at Pearcedale Primary School believe it is important to use technologies effectively and responsibly.

The use of the Internet in education can provide a number of specific learning benefits, including the development of: Independent learning and research skills (improved access of specific learning across a wide range of learning areas), Communication and collaboration- the ability to use learning technologies to access resources create resources and communicate with others, Enhance teaching and learning in several ways: for communicating with other people, for publishing students' work, for research and learning basic skills. As ICT in general is part of everyday life we need to ensure that all users acquire knowledge, understanding and the ability to use various forms of ICT throughout the curriculum.

Please Note: The term 'Information & Communications Technology' is applied to various forms of technology & communications apparatus including: computers, scanners, video units, Interactive White Boards, digital cameras, listening centres, audio and broadcasting systems, as well as web 2.0 connectivity tools on the Intranet and Internet research: websites, search engines and web browsers, mobile phones and personal digital assistants (PDAs), wireless games consoles, webcams and videoconferencing

2.0-Purpose

1. To create a climate within the school in which staff and pupils become comfortable and confident with ICT and its uses.

2. To establish developmental guidelines ensuring a coherent progression from P–6.

3. To ensure awareness of the availability of hardware and software in the school and organise these resources to address differing developmental and educational needs.

4. To create opportunities for staff and students to acquire necessary ICT skills that enhance teaching – learning relationships.

5. To establish responsibilities and procedures that promotes effective and safe practices.

3.0- Roles:

3.1-The Role of the School:

The school undertakes a commitment to provide appropriate physical resources to facilitate the successful incorporation of ICT throughout the curriculum. In addition, the school will promote and support: the up-skilling of the school community, compliance with legal requirements and the effective inclusion of ICT into the school's curriculum, through its planning and procedures.

3.2-The Role of the Staff within the school:

The school expects that each staff member will integrate ICT throughout the curriculum (as with any other curriculum resource) and provide guidance, supervision and instructions to students in the appropriate use of such resources. Staff will facilitate student access to curriculum information resources appropriate to the individual student instructional needs, learning styles, abilities and developmental levels. Staff must familiarise themselves with the Pearcedale Primary ICT Policy. This should happen at the start of each year as a part of induction. (see Appendix B). The Using Social Media Tools: Guide for Department Employees in Schools (Guide) has been developed as a practical guide to support Department employees in schools to understand and meet the obligations and behaviours set out within existing instruments, polices and guidelines outlined within the Scope of this Guide
http://www.education.vic.gov.au/school/principals/health/Pages/lolsocialmedia.aspx

3.2a-Supervision

Teaching staff are primarily responsible for monitoring ICT usage of students, including prevention of vandalism, cyber bullying, excessive web access, inappropriate websites, and so on. Students must not be permitted to use ICT resources without supervision. In cases where ongoing monitoring is required the ICT Admin can help but the first responsibility lies with the teacher.

3.2b-Incident Reporting

If a teacher becomes aware of an incident concerning abuse of E-safety issues, (including those that happen out of school hours,) they must fill out the relevant information in the e-smart incident record which is kept in the ICT Lab. (See Appendix E)

3.2c-Out of Hours Online Behaviour

Staff should be mindful of maintaining a professional online presence, both as role-models to students and as representatives of the school. Staff must not post any publicly available content on social sites such as Facebook etc., which would tarnish their professional reputation or harm the reputation of the school in any way. In addition, staff are not permitted to socially contact students through such websites, or chat programs for example, by adding students as "friends" on Facebook. This is in breach of the DEECD policy Protective Practices for Interactions with Students.

http://www.decs.sa.gov.au/docs/documents/1/ProtectivePracticesforSta.pdf

3.3-The Role of Parents:

Parents and guardians are also responsible for setting supervision and access standards that their children should follow when using media and information sources in accordance with current legislation requirements and school policy and procedures. (See Appendix A and C)

3.4-The Role of Students:

Students are responsible for appropriate use of ICT, in compliance with specific Acts and school procedures. Communications on the information networks are public and general school rules for student behaviour, conduct and standards will apply. Individual users of the school computer networks are responsible for their behaviour and communications over those networks. Students will comply with school standards and will honour the agreements they have signed. (See Appendix A and D)

4.0-Devices from home

Pearcedale Primary school implemented a 1:1 BYOD (Bring Your Own Device Program) Program for Grade 5 and 6 in 2017. Every student must sign an Acceptable Use Agreement before bringing their device to school.

Other students are not to bring electronic devices from home unless for the purpose of transporting homework. They must not bring mp3s or burned CDs from home as this could violate copyright laws. Mobile phones and other electronic devices will not be used during lessons or formal school time. All mobile phones will be signed in before the start of the day. How this will work will be at the discretion of the classroom teachers. The sending of abusive or inappropriate text messages is forbidden. School shall not be held responsible for the loss or damage of any items brought from home.

5.0-Safety

DEET has provided web filtering; the students' use is monitored and manual updates are made to the filter. However due to the breadth of content available on the Internet there is no guarantee that all unsafe material will be blocked. All efforts are made to provide a suitable internet experience for students.

Staff will supervise all internet use to ensure student safety. Staff will assess research topics and check searches beforehand to prevent inappropriate material from being shown to students. Staff should familiarise themselves with the principles of internet safety and reinforce these principles with their students. Internet safety is taught and encouraged; this means not giving out personal details on websites or in emails. Also cyber-bullying is forbidden. Students use ICT facilities while under supervision, and in the computer room students can be monitored by the teacher using software which displays their current activities either in summary form or directly showing what is on the student's screen.

6.0-Responsibilities

Parents, Caregivers and Students must read the Student ICT Usage Agreement. Parents and Caregivers must complete a permission form at the bottom of the agreement for students to access the Internet and email. Parents and Staff are to assist students to understand their responsibilities. Students must sign off that they have read and understood their responsibilities at the bottom of the Acceptable Usage Agreement. Parents must return the Parental Permission form before students are permitted access to ICT facilities.

6.1-ICT Support Staff Responsibilities

The ICT Administrator shall:
- monitor user quotas and warn users of excessive usage
- investigate excessive use and inappropriate sites and files
- block inappropriate sites using the web filter
- report inappropriate usage to the teacher and leadership, and enforce bans where appropriate
- maintain a list of user account details/passwords and update when necessary

• provide appropriate content on school intranet for use of staff and students
• monitor and investigate any irregularities in account usage

6.2-Consequences

Staff that fail to follow Pearcedale Primary and DEET ICT policies will be initially warned and counselled with regards to appropriate usage and behaviour. Continuing misconduct will be referred to Leadership for review and further action.
Students that fail to follow Pearcedale Primary and DEET policies with regards to ICT will be subject to disciplinary action including but not limited to the following:
• First offence: Warning and advice on incorrect behaviour
• Second offence: Internet Ban for a time as determined by teachers and parents notified if necessary.
• Third offence: Computer use will be restricted to offline computer only or alternate work will be found. Parents notified if deemed necessary.

Other consequences that may include:
• Suspension from ICT Activities
• Suspension from school
• Parents/guardians will be invoiced for repairs to any vandalised/damaged equipment
• Forbidden devices will be confiscated and returned at the end of the day
• Inappropriate files will be deleted
• Inappropriate websites will be blocked

7.0-Levels of Student Access

Before students are permitted to access the Internet they must be familiar with the E-Smart Student Code of Conduct. All teachers are required to explain these guidelines to their students. Students in Year 3 to Year 6 will be asked to sign a statement that they have read and understood the Code of Conduct and agree to abide by it.

Pearcedale Primary School
Acceptable Use Agreement for Internet and Digital Technologies

Pearcedale Primary School believes the teaching of cybersafe and responsible online behaviour is essential in the lives of students and is best taught in partnership between home and school.

21st century students spend increasing amounts of time online, learning and collaborating. To be safe online and to gain the greatest benefit from the opportunities provided through an online environment, students need to do the right thing by themselves and others online, particularly when no one is watching.

Safe and responsible behaviour is explicitly taught at our school and parents/carers are requested to reinforce this behaviour at home.

Some online activities are illegal and as such will be reported to police.

School support for the safe and responsible use of digital technologies

Pearcedale Primary uses internet and digital technologies as teaching and learning tools. We see the internet and digital technologies as valuable resources, but acknowledge they must be used responsibly.

Your child has been asked to agree to use the internet and mobile technologies responsibly at school. Parents/carers should be aware that the nature of the internet is such that full protection from inappropriate content can never be guaranteed.

At Pearcedale Primary School we:

- have policies in place that outline the values of the school and expected behaviours when students use digital technology and the internet
- provide a filtered internet service.
- provide supervision and direction in online activities and when using digital technologies for learning
- support students in developing digital literacy skills
- have a cybersafety program at the school which is reinforced across the school
- use mobile technologies for educational purposes (e.g. podcasts or photos from excursions)
- provide support to parents/carers to understand this agreement (e.g. language support)

- provide support to parents/carers through newsletters and through the document attached to this agreement for parents to keep at home
- work with students to outline and reinforce the expected behaviours.
    - reinforce that cybersafe and responsible behaviours are expected.

Student Agreement

When I use digital technology I agree to:

- get permission from a teacher before using a computer or other ICT equipment
- be a safe, responsible and ethical user whenever and wherever I use it
- support others by being respectful in how I communicate with them and never write or participate in online bullying (this includes forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviour)
- talk to a teacher if I feel uncomfortable or unsafe online or see others participating in unsafe, inappropriate or hurtful online behaviour
- seek to understand the terms and conditions of websites and online communities and be aware that content I upload or post is my digital footprint
- protect my privacy rights and those of other students by not giving out personal details including full names, telephone numbers, addresses and images
- use the internet for educational purposes and use the equipment properly
- use social networking sites for educational purposes and only as directed by teachers.
- Understand that the use of Google Apps for Education is limited to school related activities only
- abide by copyright procedures when using content on websites (ask permission to use images, text, audio and video and cite references where necessary)
- think critically about other users' intellectual property and how I use content posted on the internet.
- not interfere with network security, the data of another user or attempt to log into the network with a user name or password of another student
- not reveal my password to anyone except the system administrator or the teacher
- not bring or download unauthorised programs, including games, to the school or run them on school computers

When I use a mobile phone, iPod or other mobile device I agree to:

- keep the device off during school times and only make or answer calls and messages outside of school times – except for approved learning purposes. Note: You may be required to sign your mobile in with your classroom teacher
- protect the privacy of others and never post or forward private information about another person
- only take photos and record sound or video when it is part of an approved lesson
- seek permission from individuals involved before taking photos, recording sound or videoing them
- seek appropriate (written) permission from individuals involved before publishing or sending photos, recorded sound or video to anyone else or to any online space
- be respectful in the photos I take or video I capture and never use these as a tool for bullying

This Acceptable Use Agreement also applies during school excursions, camps and extra-curricula activities. I acknowledge and agree to follow these rules. I understand that my access to the internet and mobile technology at school will be renegotiated if I do not act responsibly

Consequences for failing to follow this agreement include but are not limited to:
Students that fail to follow Pearcedale Primary and DEET policies with regards to ICT will be subject to disciplinary action including but not limited to the following:
• First offence: Warning and advice on incorrect behaviour
• Second offence: Internet Ban for a time as determined by teachers and parents notified if necessary.
• Third offence: Computer use will be restricted to offline computer only or alternate work will be found. Parents notified if deemed necessary

Other consequences that may include:
• Suspension from ICT Activities
• Suspension from school
• Parents/guardians will be invoiced for repairs to any vandalised/damaged equipment
• Forbidden devices will be confiscated and returned at the end of the day
• Inappropriate files will be deleted
• Inappropriate websites will be blocked

Student

I understand that if I do not abide by the Code of Conduct my right of access to computers will be restricted or withdrawn. I understand the rules for using the Internet and agree to abide by them. I understand that any breach of these conditions will result in internet and mobile technology access privileges being suspended or revoked.

Name (printed)

Signature Class

Date

I agree that I have read and discussed the Student Usage Agreement with my child and will support the application of these rules.

Signed

Parent/Caregiver's name

If you have any concerns about this agreement or ideas for making the agreement better contact school

For further Support with online issues students can call Kids Helpline on 1800 55 1800. Parents/cares call Parentline 132289 or visit http://www.cybersmart.gov.au/report.aspx

Appendix-b

Acceptable Use Agreement-Staff

The school has provided computers for use by staff. They offer access to a vast amount of information for administrative and school management purposes offering great potential to support the school. The computers are provided and maintained for the staff, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Do not install, attempt to install, or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes, e.g. buying or selling goods.
- Do not open files brought in on removable media (such as floppy disks, CDs, flash drives etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not eat or drink near computer equipment.

Security & Privacy

- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number or your school's name, or send them your picture.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas will be treated like school lockers. Staff may review files and communications to ensure that users are using the system responsibly.

Internet

- Do not access the Internet unless for school activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed,
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of the senior leadership team.

Please read this document carefully. If any teacher violates these provisions, access to the Internet will be denied and the staff member will be subject to disciplinary action.

Staff' Internet Code of Practice.

- Staff should be familiar with the school's Network, Internet, e-mail and web site creation policies and the pupils' code of practice for Internet use.

- Staff should closely monitor and scrutinise what their pupils are accessing on the internet including checking the history of pages.

- Computer monitor screens should be readily visible for the teacher, so they can monitor what the pupils are accessing.

- Pupils should have clear guidelines for the content of e-mail messages, sending and receiving procedures.

- Use of the Internet should be supervised by a teacher or adult.

- Pupils should be taught skills and techniques to enable efficient and effective use of the Internet.

- Pupils should have a clearly defined focus for using the internet and e-mail.

- If offensive materials are found the monitor should be switched off, any printed materials or disks should be confiscated and offensive URLs should be given to the IT Co-ordinator who will report it to the Internet Service Provider.

- Virus protection has been provided by the school as viruses can be down loaded accidentally from the Internet. Pupils bringing work from home, on USB sticks, could also infect the computer.

- The recommended ISP will check sites visited by schools.

- It is recommended that pupils do not use open forums such as newsgroups or chat rooms.

- Disciplinary action may be taken if the Internet is used inappropriately e.g. for accessing pornographic, racist or offensive material for personal financial gain, gambling, political purposes or advertising.

- Software should not be downloaded from the Internet (including screen savers, games, video clips, audio clips, *.exe files).

Staff will read the Code of Practice for pupils and staff and become familiar with the school's policy on the use of the Internet, e-mail, the creation of web sites and network security.

Appendix-c

Information to Support Parents with Cyber Concerns

Parents of children at Pearcedale Primary should aim to be involved and aware when it comes to their children's use of technology. While it can be challenging for parents to keep abreast of the dynamic nature of the internet and the use of computers and other mobile devices, there are steps parents can take to equip themselves with improved knowledge and awareness and where to access for assistance if required.

The information below has been designed to assist parents as a starting point although this information is by no means comprehensive. Please take the time to explore some of the links provided and consider the issues raised.

What are parents' biggest concerns?

Clearly the answer to this question varies among individuals. However, some common concerns that parents have of their children involved in the cyber world are:

- **Predators** – parents are stunned at the lengths sexual predators will go to in an attempt to corrupt children and how easy it is to access information. Getting involved with a predator online is usually done so by children with no knowledge whatsoever of whom they are really talking to. Parents should educate children not to communicate with anyone online whom they do not already know. If parents suspect that communication is occurring with a stranger, they should take steps to end all communication, and if any element of danger is suspected, it should be reported to the police.

- **Bullying, harassing, stalking** – quite simply this has become one of the most concerning misuses of new technology. One of the biggest changes with bullying today is that now it is almost inescapable, even in the privacy of a child's own home. Parents should insist that mobile phones are left on the kitchen bench at night and not allowed in a child's bedroom, and likewise, with internet use, i.e. keep it out of bedrooms.

- **Privacy, identity theft -** Children don't appreciate the ramifications in sharing their password or giving out information that may result in a breach of not only their personal information, but that of the whole family. Identity theft occurs more frequently than many parents may realise; the perpetrator is often someone who our children know, not just strangers. Children should never use known passwords or password hints such as pet's name, middle name and so on. Internet filters can assist with these restrictions.

- **Pornography**- Even very young children can encounter pornography on the internet even when they are not searching for it. This vulnerability is a concern for parents of all ages. Older children risk serious repercussions if involved in viewing pornography and are not aware of this in many cases.

- **Pop-ups & spyware** - One of the concerns with a child's natural curiosity is that they enter sites that contain embedded spyware and viruses and downloading that song (often illegally) might seem like a good idea, but can come at a greater cost than they realise.

- **Social chat sites** - most parents are aware of Facebook, Myspace, MSN as social chat sites, however, many parents are not aware that dozens of other sites exist and their children are using many of these. Further, some students have multiple accounts and therefore passwords, so what a parent may see, may not be the full picture.

- **Feeling of uselessness** – many parents feel that they simply cannot keep up with the rapid pace of technology and therefore, it becomes just all too hard. While it is easy to feel overwhelmed, there are many life skills and experiences parents do have that are of tremendous benefit to children.

What you can do as a Parent? Here are some helpful points.

- Give yourself the best chance of being aware and limiting temptation by setting the computer in a common family place such as a living room. It is not recommended for children to have a computer in the bedroom if they have access to the internet. Further, remain proximal when your children are using their computer and know what sites they are using by talking to them and setting boundaries and expectations.

- Set rules and limitations related to all areas of technology. Pay particular attention to the use of social networking sites where virtually all cyber-bullying is generated. A good idea is to sit with your children while they are using the site and read the dialogue. Your child will probably not be very receptive to this idea; however, this will have a big influence on what they write and what their friends write.

- If your child is being bullied, firstly support them, rather than portion blame in any direction. Encourage your children to communicate with the school, with your support to get the situation "on record". Schools have an obligation to protect children and all cases of bullying are followed up at Pearcedale Primary School. If you feel we as a school have not done so, please ensure that you communicate with us about your concerns so that further follow up can take place where appropriate. Many children feel that reporting bullying will result in making it worse in the short term. However, if it is not reported there is little reason for the bullying to stop. Evidence shows that reporting bullying and skilful application of the process by the school and parents provides the best outcomes for children being bullied. Importantly, be objective and ensure you print off or record all correspondence and/or conversations online from all parties and present them to the school. Our experience as a school suggests that virtually all cyber-bullying is sent from the home environment with parents having no idea what their child is writing.

- Consider possible consequences to irresponsible behaviour in advance. Sometimes children do not want to report to parents when they get into genuine difficulty as they perceive the technology will be removed as a consequence. It is worth communicating not only expectations of use, but also consequences as well, so that communication between children and parents remains open. Encourage them to report to you any time they feel unsafe or threatened when using the internet.

- Remember that mobile devices with internet access (very common) have equal power to that of a computer, and further still, proxy access to certain sites is possible, even when regular access is cut off from parents. Monitoring the use of a mobile device is equally important as that of the computer itself. Ensure they are left on the kitchen bench

overnight and not taken into private rooms, as children and teens cannot help but look at all incoming information.

How to Prevent Your Child from Being Victimised

- **Be your child's support system.** The biggest way to prevent your child from being a victim is to keep the lines of communication open. The means walking a fine line between a concerned caregiver and an overprotective parent. Your child needs to feel that he or she can come to you without negative repercussions. If they are afraid you'll ban them from the Internet or keep them from going out with friends, they will not confide in you. It also means listening carefully and avoiding the tendency to trivialise what they are experiencing. It may not seem like a big deal to an adult that the most popular kids in school made fun of your child's hair or clothes, but it can be a serious blow to the self-esteem of a child or teen.

- **Be firm.** Set rules regarding when and how long your child can be online. Accessing the Internet is akin to inviting someone into your home, so you may choose to only allow Web time when you're at home. Use Internet filters, timers, and whatever else you need to do to protect your child.

- **Know your child.** This is very important. Kids who are already suffering from low self-esteem or depression are prime targets for cyber-bullying. It can be tempting to assume that your child is just going through a phase or that they're just in a "bad mood," but you are better off seeking professional help if there is a problem than simply waiting things out. Look for opportunities to speak and discuss things with your child "as a friend" rather than in "parent mode" and when both parties are relaxed.

- **Know the danger signs.** Your child may become more withdrawn or moody. They may spend more time online, or may refuse to use the computer altogether. They may cut off ties with friends. If your child gives any indication that they are being bullied on or offline, take it seriously.

- **Educate.** Teach your child what to do in cases where they feel threatened or bullied. They should ignore the offender and contact an adult immediately. They should never engage with the person who is threatening them as that is only encouragement for the behaviours to continue. As an adult, if you feel threatened by someone online, contact the police just to be safe. You can also use built-in measures on certain websites, such as ignoring or reporting someone else.

- *Source:*
http://familyinternet.about.com/od/computingsafetyprivacy/a/cyberbully.htm

For more information on all above issues.

Please read further on:

For specific information on cyber bulling and general concerns:

http://www.kidspot.com.au/

http://www.stopcyberbullying.org/parents/parents_biggest_concerns.html

ACMA: Cybersmart Kids Online

A user friendly site for children and parents to find out how to be cyber smart and safe.
www.cybersmart.gov.au

Click: A Technology Guide for Parents

This NSW Government Information Communications Technology (ICT) Guide for parents has been developed to help parents protect their children at home or when they are out with friends. It provides comprehensive information including cyber bullying and will be regularly updated with new developments in the ICT industry and in our schools.

www.schools.nsw.edu.au/media/downloads/schoolsweb/news/technology/click.pdf

Cyber bullying, e-crime and the protection of children

A pamphlet for parents and caregivers that includes advice about what to do if your child is feeling unsafe following online or mobile phone communications, or exposure to offensive internet sites. From SA's Department of Education and Children's Services.

http://www.decs.sa.gov.au/docs/documents/1/CyberBullyingECrimeProtec.pdf

Cybersmart Information for Parents

Brochures, tips, guides and a poster from the Australian Communications and Media Authority

http://www.cybersmart.gov.au/Parents/

Source: http://www.bullyingnoway.com.au

Appendix-d

Information for Students to Remain Cyber-Safe

There are a number of steps you can take to increase safety and reduce risks associated with the cyber world. While not every possible individual scenario can be considered in this document, many practical tips have been included. You are encouraged to make recommendations to enhance the effectiveness of this page so as to support each other in remaining safe when online.

Some practical tips for students:

- Never **set hints to passwords** to obvious answers such as your pets name, middle name or favourite 'things'. Only use hints that no-one else could possibly know the answer to, not even your best friend. Never share your password and change it regularly.
- While your friends are your friends, it is important you never give them your password, not even once. Do not give your password even to your best friend! Your password allows you to enter your computer, and shouldn't let anyone else access your account. Do not give your password to anyone regardless of how well you think you know them.
- Ensure that social internet sites are set to 'private' setting at all times and check periodically, especially after 'updating' information where they can be reset back to 'public' viewing. For example: Facebook sometimes does this so it is wise to check your password security settings on a regular basis. Do not enter your school name when entering Facebook or other sign up information – this is to protect your privacy.
- Do not make available any information online that you would not tell a stranger in the street. Effectively, it is the same!
- Never 'chat' to strangers you meet online, in some instances they are not who they say they are, and in some cases they are dangerous criminals pretending to be someone your age.
- Leave your mobile phone in the kitchen at night when you sleep and study. It is a distraction you do not need!
- Only use the internet in a common place in the family home, not your bedroom. You are less likely to be tempted to waste time or engage in conversations you know you should not be involved with.
- **Know the law!** If you send an email or text to a friend, be aware that they are classed as a public document and it is not a private message.
- **Know the law!** There are anti-harassing, bullying and stalking laws in state and at a Federal level as well. You can potentially be charged with a crime if you send threatening, bullying, intimidating or sexually suggestive messages to another person.
- Be aware! If you upload any photo of yourself of friends, it is likely that they will be copied by others and therefore, available on the internet for the rest of your life. It has been suggested by one major social site that photos are copied on average 11

times every 24hours online! Ask your friends in the photos for their permission to upload the photos; they may not want the world to have access to them.

- Downloading music from sites such as 'LimeWire' etc., increase the risk of your computer being targeted with spyware and viruses as you are getting pieces of information from many sources of personal computers around the world, not a 'safe' online company. This can destroy your computer and all files on it. This could also be contravening Copyright laws and robbing the music industry of its income.
- Invest in and install a good anti-virus program to protect your computer. This software should be able to alert the user of a contaminated file and stop any 'nasties' from infiltrating and/or destroying your files. Set the virus software to scan the computer on a regular basis.
- If you are being bullied or receive a threatening type message, always print it off and save it, and report it to teaching staff at Pearcedale Primary School promptly. Our experience is that if you don't report it, then it is likely to continue. If you do report it, steps will be taken by the school to support you. Do not reply to them at all or you could make the situation worse!
- Beware that joking around or about your friends is fine if they are up to it and if it is a one off jest, however, be careful it does not become a regular habit to the point they feel bullied.
- Only open email or chat to people you know on the internet. If anyone you don't know wants to meet, or asks you to send them your photo, report it immediately to an adult such as your parents or teachers.

Appendix-e

E-Smart- Incident Record

Name of student	Type of incident	Date Informed	Where incident occurred
eg. A Smith	Mutual conflict: random acts of aggression or intimidation	12/02/11	Playground

Incident	Where	Other students	Response	Staff	Parent informed	Meeting	Resolution
Mutual conflict: mutual arguments and disagreements	Classroom	Involved in incident as perpetrator	Private interview at the time	Incident managed by yard duty or classroom teacher	Phone call		Teacher interview
Mutual conflict: single episodes of social rejection or dislike	Playground	Reported incident	Meeting arranged	ICT Coordinator	Email		Mediation
Mutual conflict: single-episode acts of nastiness or spite	Lab	Involved in incident as bystander	Immediate sanctions imposed	Assistant Principal	Letter		Restorative conference
Mutual conflict: random acts of aggression or intimidation	Library	Other involvement	Other restorative approach	Principal involved	Parent not informed		Recess or lunchtime detention
Cybersafety	Travelling to/from school		Positive Behaviour Support				
Cyberbullying	Via technology		Detention				
Unacceptable or inappropriate use of technology			Suspension				
Other			Exclusion				

Other student involvement	Response	Staff Involved	Parents informed and Date	Action Required
Involved in incident as perpetrator	Private interview at the time	J. White	Phone call	Meeting With Parents
