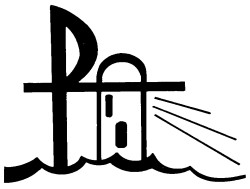


CYBER-SAFETY GUIDELINES FOR SCHOOLS

DRAFT VERSION 2.5

CONTENTS

CYBER-SAFETY GUIDELINES FOR SCHOOLS

INTRODUCTION

The focus of our Diocesan Schools System Strategic Plan *Going Forward Together 2007-2010* is on students. Parents can be confident that their Catholic schools are continuing to provide quality Catholic education in a safe and nurturing environment, equipping students to make a difference in the world as disciples of Jesus. In striving to achieve this goal schools will work in partnership with parents and parishes. This is especially important when using the Internet and other digital technologies where the boundaries between the classroom, the playground and the home tend to overlap considerably.

There is no doubt that the Internet and digital technology in general offer an enormous range of opportunities for today's children. They are growing up in a digital environment which provides the capability for instant online communication, information discovery and online publishing. Perhaps more so than their parents and teachers, children are very comfortable with this technology and they readily embrace and adopt the new technological developments which seem to come along at an ever increasing pace. Not surprisingly then, students in our schools have been labelled *The Net Generation* or *Digital natives* and the electronic media are their social lifeblood.

While embracing many of the opportunities presented by the Internet, Pope John Paul II did warn about some aspects of its ephemeral nature and the flood of information provided by the Internet:

"The Internet offers extensive knowledge, but it does not teach values; and when values are disregarded, our very humanity is demeaned and man easily loses sight of his transcendent dignity. Despite its enormous potential for good, some of the degrading and damaging ways in which the Internet can be used are already obvious to all, and public authorities surely have a responsibility to guarantee that this marvellous instrument serves the common good and does not become a source of harm." [1]

Pope Benedict XVI has also spoken about the need to safeguard children and families from the dangers of the Internet.

"On the one hand, undoubtedly, much of great benefit to civilization is contributed by the various components of the mass media," he said. "On the other hand, it is also readily apparent that much of what is transmitted in various forms to the homes of millions of families around the world is destructive."[2]

Similarly, the Australian Catholic Bishops' Conference, in its Pastoral Letter on Internet Safety, acknowledges the many benefits of the Internet and digital technology in general but also draws our attention the dangers they present if they are not well managed.

---

[1] Pope John Paul II, "Internet: A New Forum for Proclaiming the Gospel", n 2.

[2]

2 Pope Benedict XVI, "Address to Plenary Council of the Pontifical Council for Social Communications", March 9, 2007, accessed at http://www.zenit.org/article-19115?l=english on February 20, 2008.

"Parents, educators, Church leaders, psychologists and others are raising concerns about the dangers of the Internet"

"it is the Church's firm view that the Internet should be no more exempt than other media from reasonable laws against hate speech, libel, fraud, pornography – especially child pornography, and other offences."

A Pastoral Letter from the Catholic Bishops of Australia

The Australian Bishops Conference also acknowledges that concerns about Cyber-safety need to be addressed through the *"context of Faith".*

In terms of legislation, both the Commonwealth and State Governments require that schools take appropriate measures to ensure that the use of digital technology by students does not place them at risk. The regulations associated with the *Schools Assistance (Learning Together – Achievement Through Choice and Opportunity) Act 2004* state that all schools are required to implement the National Safe Schools Framework. Catholic School Systems are required to report each year, through the CEC NSW that their schools comply with this requirement.

At the state level, the Education Act 1990 makes explicit the responsibilities of schools and school systems in relation to the provision of a 'safe and supportive environment'. The details of these requirements are contained in Sections 5.6.1 and 5.6.2 of the *Registration Systems and member Non-government Schools (NSW) Manual.* Compliance with these requirements, which include by their very nature matters pertaining to Cyber-safety, is required for systems to retain their status as legal entities which register and accredit member schools.

The vision statement of the **National Safe Schools Framework** is quite straightforward: **"All Australian schools are safe and supportive environments."** The Framework provides six *Key Elements* which can be used as an initial checklist for school communities to use in assessing the comprehensiveness of their approach to establishing a safe and supportive environment which includes Cyber-safety. The Key Elements are:

School values, ethos, culture, structures and student welfare

Are values which contribute to maintaining a safe and supportive learning environment shared across the school community?

Is social justice a core part of the school's ethos?

Is the culture of the school a positive and inclusive one which values the contributions of all members of the school community equally?

Establishment of agreed policies, programs and procedures

Are there clear definitions of harassment, bullying, violence and child protection available which are known and understood by all members of the school community?

Are there clear policies programmes and procedures in place for preventing and responding to harassment, bullying, violence and child abuse and neglect which are known and understood by all members of the school community?

Provision of education and training to school staff, students and parents

Are all staff well-informed and kept up to date about harassment, bullying, violence and child protection, and trained in appropriate prevention and response strategies?

Are all students accessing age appropriate information about harassment, bullying, violence and child protection?

Are all parents and carers informed about harassment, bullying, violence and child protection and able to engage in school planning?

Managing incidents of abuse and victimisation

Are there clear and well-understood processes for reporting and managing incidents of abuse and victimisation?

Are all members of the school community encouraged to identify and report cases of abuse and victimisation using agreed processes?

Are there strong and established relationships with relevant specialists to provide support for staff dealing with cases of child abuse?

Providing support for students

Are there strong and established relationships with relevant specialists to provide support for students affected by victimisation or abuse/neglect?

Working closely with parents

Are parents closely involved in preventing harassment, bullying and violence, and informed and consulted when their own children are involved in incidents?

Are parents encouraged and supported to promote confidence in their children and to develop open relationships with them?

PURPOSE

These guidelines provide direction for the implementation of Cyber-safety technical and educational processes for staff and students in the Diocesan School System (DSS) of the Diocese of Broken Bay. The Cyber-safety Guidelines for Schools support the wider implementation of the "Creating Safe and Supportive School Environments – Child Protection Policy for Diocesan Systemic Schools".

The use of the Internet in schools needs to be managed in such a way that students are able to access content that is appropriate for their stage of development and relevant to their education.

In accessing the Internet, staff and students are expected to conduct their activities in a manner that supports and advances the mission of Catholic schooling in the Diocese, the education and formation of students in Catholic discipleship and respects the dignity, rights and privacy of all persons.

DUTY OF CARE

The DSS acknowledges that the Digital Education Revolution will provide greater opportunity for staff and students to engage in 21st Century learning experiences, and that more often than not will involve increased on-line activity and engagement, as well as the use of connected digital devices.

Such activity may include, but is not limited to, email and chat, video conferencing, internet browsing, digital content creation, telephony and exposure to Web 2.0 technologies.

The DSS acknowledges that it has a duty of care to staff and students in ensuring that engagement in on-line learning and communication is carried out with the utmost concern for personal safety, security, and privacy. The DSS acknowledges that parents, children, and young people have a need for knowledge around the potential risks involved in on-line learning and communication. It seeks to support parents, in their role as prime educators of their children, by taking an active role in disseminating information and the provision of educational opportunities.

It is important that we acknowledge that threats to our safety, human dignity, and relationships with others and with God can manifest themselves within the digitally connected world of the 21st Century. Some of these threats include the following:

- Unwelcome Websites
- Stranger Danger
- Cyber-bullying
- Financial Exploitation
- Unlawful Use

Unwelcome Websites are often encountered when students search for information utilising Internet Search Engines such as Google, Altavista etc. These websites often contain material that may be age inappropriate, contain sexually explicit and or pornographic material, violent and offensive.

Stranger Danger, a term that is familiar for most adults, exists on the World Wide Web. Paedophiles and other people who may wish to hurt children use the Internet to search for potential victims. Often these people pretend to be someone other than who they really are to establish inappropriate relationships on-line that may result in a physical meeting of some description.

Cyber–bullying that manifests itself on the Internet can have devastating effects for the victim and their family. Cyber-bullying is not limited to but may include teasing, spreading rumours, making fun of someone, threats, and exclusion from social circles. It is not limited to the Internet and may be carried out through SMS/Mobile.

Financial Exploitation is made possible through the harvesting of personal information that may include credit card and mobile phone account details through the use of cleverly disguised websites and other downloaded programs e.g. Trojans and viruses.

Unlawful use may arise through the misuse of the DSS Network. Some examples of this may include the downloading and distribution of mp3 and movie files through Peer to Peer networks.

In meeting this challenge the DSS will:

- Provide content filtering and monitoring for all school sites;
- Support schools in the implementation of a system-based Cyber-safety Statement;
- Provide ongoing support to schools in educating staff, students and parents about Cyber-safety.

RESPONSIBILITY

The Catholic Schools Office works in partnership with schools to provide technical and educative resources that aim to minimise the risk of harm that is sometimes associated with learning in the digital age.

Technical Resources that are deployed at the DSS level provide the following:

- Central Content Filtering through the Catholic Education Network (CENET);
- SINA School-based Content Filtering; and
- Support for the tracking and Logging of user activity;

Central Content Filtering is provided for all diocesan schools by the Catholic Education Network (CENET). CENET provides an overarching content filtering system that is based on categorisations and is deployed by way of a Secure Web Smart Filter. This level of filtering utilises a database of over 20 million blockable websites in over 91 categories.

School-based Content Filters are monitored and maintained through the SINA interface by the schools SINA Administrator. These filters provide the technical capacity to block access to sites based on category and or web address as well as the capability to filter email reception.

User activity may be tracked and logged by the DSS as part of the conditions of the Acceptable User Agreement for DSS Network Services.

Each school in the diocese of Broken Bay has a staff member who is the designated SINA Administrator. The SINA Administrator supports the Principal in maintaining a "safe and supportive" on-line environment for students and staff.

The SINA Administrator is responsible for the:

- Creation, Modification and Deletion of user accounts;
- Monitoring and updating of school-based filters;
- Monitoring and reporting of user based reports.

Educational and Policy based support for schools include:

- Child Protection - "Creating Safe and Supportive School Environments"
- Child Protection - "Protective Behaviours"
- PDHPE – Interpersonal Relationships Strand (Stages 1-3)

Diocesan Schools will:

- Implement school-based Cyber-safety programmes and communicate the content and format of such programmes to their school communities.
- Support staff in the development of educational programmes, activities, and promotions that are explicit in their approach to equipping students with knowledge, understanding and strategies to improving their Cyber-safety skills;
- Manage & monitor all Internet traffic in accordance with Diocesan policy; and
- Maintain a register of Cyber-safety Incidents.

SCHOOLS INTERNET / EMAIL MONITORING

All Diocesan Schools are responsible for maintaining and auditing Internet and network access records. The SINA Management Interface may be used to capture information about network traffic, websites visited, web searches conducted and to maintain the individual school-based filters.

The Principal, or delegated authority, is responsible for ensuring that monthly audit reports are collated and archived for future reference.

Reports that will be retrieved and archived include:

- School-based Summary Report (monthly)
- Access Denied (monthly)
- Top 100 Sites (monthly)

The *School-based Summary Report* contains information about the volume of internet and email traffic, disk usage, school costs and breaches. Whilst all of this information is useful to SINA Administrators and Principals, of particular importance is the information contained in the “breaches” detail. The “breaches” detail provides the total number of breaches logged for the school over the period of a month. It is expected that SINA Administrators would use this information to perform an “Access Denied” search to identify individuals, when appropriate staff, who have logged “breaches”. After identifying individuals, the SINA Administrator or Principal, may then initiate discussion with them that is aimed at effecting a change in behaviour. This may include reference to the Network Services Policy and Acceptable User Agreements.

The *Access Denied Report* will assist in identifying users who may have tried to access materials that have been deemed inappropriate by the main Central Filters (CENet) or the School-based Filters. The Principal, or delegated authority, may choose to investigate any breaches under the terms of the School-based Acceptable Use Agreement or the DSS Network Services Policy.

The *Top 100 Sites Report* will identify the most popular websites visited by each school for the previous month. SINA Administrators, in collaboration with Principals, may utilise this information in decision making processes around the blocking and monitoring of websites that pose risks to student and staff safety.

The outcome of any investigation conducted may result in privileges being withdrawn from the user(s) as described in the DSS Network Services Policy.

REGISTER OF CYBER-SAFETY INCIDENTS

All Diocesan Schools are responsible for maintaining a Register of Cyber-safety incidents that occur. Information may be recorded manually or via Student Management Software. Records contained in the register will be reviewed regularly in terms of frequency and mode of incidents. Schools may utilise this information to inform other educational initiatives if appropriate.

RESPONSE TO CYBER-SAFETY INCIDENTS

All DSS Schools will respond to pro-actively to student behaviour that breaches the Acceptable User Agreement for Internet and Network Services with reference to the following policies:

- Internet & Network Services Policy
- Student Discipline Policy
- Pastoral Care Policy
- Anti-Bullying Policy
- Ant-Harassment Policy

Appropriate action may include the withdrawal or rights to use the Internet and Network Services, Suspension, Expulsion, and the involvement of the Police.

MOBILE PHONES

All Diocesan schools will be responsible for developing and communicating their own school-based plan for the management of student mobile phones.

The DSS acknowledges that mobile phones are necessary tools for communication and learning in the 21st Century. Mobile Phones are able to store and capture data including text, images, sound and video.

Mobile Phones may pose threats to student welfare and management in terms of the capacity to engage in cyber-bullying and other illegal activities. For this reason it is advisable to communicate the following understandings to students and parents:

- students who bring mobile phones to school or on educational excursions do so at their own risk;

- mobile phones brought onto premises must be switched off upon entry to the school. They must remain switched off until the student leaves at the end of the day or unless requested by members of the teaching staff to do otherwise.

- Mobile phones may be confiscated from students who are unable to follow the school's expectations.

- In the event that it is suspected that images or videos of other students /teachers have been recorded or that inappropriate content is stored on the device, the Principal or another staff member nominated by the Principal may inspect the contents of the phone and take appropriate action that may include contacting parents or informing the Police.

The DSS acknowledges that advances in mobile phone technology make it possible to connect a mobile phone to the DSS Wireless Network. Typically a user might want to be able to do this for the purposes of gaining mobile internet access, email, and synchronization of files/calendars.

The DSS Wireless Network supports the connection of Windows Mobile Enabled Devices only. Principals, Assistant Principals, and Deputy Principals wishing to utilise this aspect of network functionality will need to request access configuration through the ICLT Services Desk. Mobile enable devices that are connected into the DSS Wireless Network will be treated as “other connected devices” whilst on the network.

No student will be permitted to connect a mobile phone to the DSS Wireless Network.

OTHER CONNECTED DEVICES

Digital Assistants, USB memory sticks, thumb drives, portable hard drives, pen drives and MP3 players may provide students with a portable form for the storage of large amounts of data. Schools must consider the threats of virus transfer, distribution of illegal or unlicensed software, images, video and music, as well as the possibility to run software before permitting them to be connected in any way (physically, wirelessly, Blue Tooth, or Infra Red) to property owned by the school.

For these reasons it is advisable to communicate the following understandings to students and parents:

- students who bring other connected devices to school or on educational excursions do so at their own risk. The school will not accept responsibility for lost, stolen or damaged devices.;

- other connected devices brought onto premises must not be connected to any property owned by the school without obtaining permission from a member of staff;

- In the event that it is suspected that images or videos of other students /teachers have been recorded or that inappropriate content is stored on the device, the Principal or another staff member nominated by the Principal may inspect the contents of the device and take appropriate action that may include contacting parents or informing the Police; and

- Connected devices may be taken and accessed if it is believed that there has been or may be a breach of the school rules or a school policy or that there may be a threat of harm to a student, another/others or system security.

SYSTEM BASED SUPPORT FOR SCHOOL COMMUNITIES

The Catholic Schools Office, Diocese of Broken Bay recognises the need to provide ongoing support for students, staff, and parents in the area of Cyber-safety. Support for school communities in relation to their endeavours to promote Cyber-safety will include, but is not limited to, the following:

- the provision of support materials for distribution to staff, students and parents;
- the facilitation of Cyber-safety Parent Forums, on request, to be held in nominated secondary school clusters;
- the facilitation of staff and leadership team meetings;
- the facilitation of Cyber-safety information sessions within the context of Staff Development Days;
- the facilitation of Cyber-safety Information Sessions at Parents & Friends Association Meetings;
- the provision of advice to school leadership teams as requested;
- the provision of on-line Cyber-safety support and educational materials
- the provision of educational materials for insertion into the school newsletters.

RECOMMENDED START OF SCHOOL YEAR PROCEDURES

EARLY TERM ONE

- Distribute newly revised Acceptable User Agreements (AUA) to all staff and students.

    - *Primary Schools*: Classroom Teachers collect, mark off on a roll sheet, and bundle agreements for archiving. Assistant Principal to assist with archiving.

    - *Secondary Schools*: Option One: Home Room Teachers collect, mark off on a roll sheet, and bundle agreements for archiving. Assistant Principal to assist with archiving. Option Two: Home Room Teachers ensure that the AUA that is contained in the College Diary has been signed.

    - *All Schools*: Assistant Principal collects, collates and archives staff Acceptable User Agreements

- *SINA Administrator* ensures that the following is in place:

    - Any generic accounts that exist in SINA are deleted or disabled.

    - Disable the accounts of students who have not returned their AUA.

    - Accounts of students and/or teachers who have left to school are migrated into the “Past Accounts” group.

    - Create new accounts for new students/teachers and ensure that they are added to the correct groupings.

    - Activate Cost Control for each group of accounts. The suggested amount per term is $40 per account for students and $40 per account for teachers. (50c per MB)

    - The SINA reporting mechanism has been configured to generate the school-based Summary Report, Accessed Denied Report and Top 100 on a weekly basis.

- Classroom and Homeroom Teachers provide orientation to the students that covers the following:

    - Implications of the Acceptable User Agreements;

    - Overview of what students must do if they encounter any of the following whilst using the DSS network

        a) Unwelcome Websites

        b) Stranger Danger

c) Cyber-bullying

d) Financial Exploitation

e) Unlawful Use

- Overview of the school's protocol that deals with connected devices. This might include, but is not limited to some of the following:

a) Mobile Phones

b) Portable Storage Devices

c) Portable Digital Assistants

d) Other connected devices

- Classroom/Homeroom teachers complete, sign and return the Cyber-safety confirmation sheet to the Assistant/Deputy Principal for collation and archiving.

- SINA Administrator accesses and stores a copy of the following reports for archiving, in a safe place, at the end of each week:

  - SINA Activity Report (forwarded via email)

  - Accessed Denied Report for the week

  - Search Engine Request Report for the week.

- SINA Administrator analyses the three reports and communicates any concerns, in writing, to the Assistant Principal/Principal for consideration of intervention or disciplinary action that might need to be taken.

Cyber-safety Confirmation Sheet

School: St. Someone's Catholic School, DBB

Year Group / Class:

Class/Homeroom Teacher:

☑ I confirm that I have facilitated a Cyber-safety Session for the students in my class/homeroom and that the content of the session included the following:

- Implications of the Acceptable User Agreements and Cost Control Administration;
- Overview of what students must do if they encounter any of the following whilst using the DSS network
    - Unwelcome Websites
    - Stranger Danger
    - Cyber-bullying
    - Financial Exploitation
    - Unlawful Use
- Overview of the school's protocol that deals with connected devices. This might include, but is not limited to some of the following:
    - Mobile Phones
    - Portable Storage Devices
    - Portable Digital Assistants
    - Other connected devices

☑ I confirm that an ACMA Cyber-safety Poster is displayed in a prominent position in the learning area that was used.

Signed:
Dated:

CYBER-SAFETY RESOURCES FOR SCHOOL COMMUNITIES

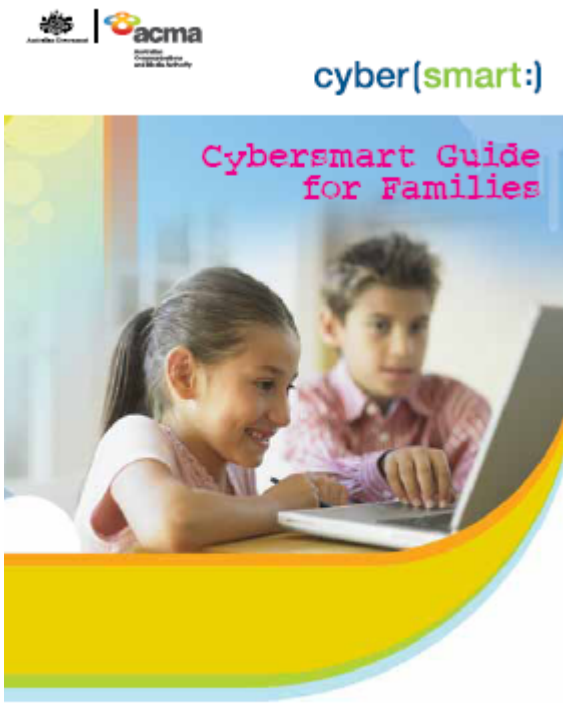
The DSS encourages partnership with parents in all aspects of school life. In acknowledging this commitment, the DSS will provide a range of Cyber-safety resources that include, but are not limited to the following:

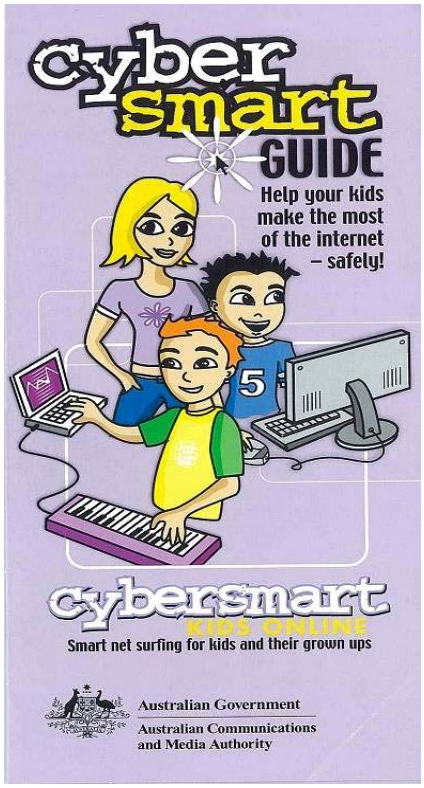
On-Line Resources

A range of Cyber-safety resources are available for access by students and teachers in an on-line mode. These resources are accessible through the Curianet Intranet Site and also through the Editure System.

The resources provided include:

- Educational materials provided by the Australian Communications and Media Authority (ACMA);
- A range of media articles and multimedia;
- Links to Cyber-safety Learning Objects;
- Cyber-safety Information Sheets provided by ACMA;





Parent Resources

A range of Cyber-safety resources are available for parents through their school office. These include past publications from Netalert and current publications produced by ACMA.

Copies of materials used in the Cyber-safety Forums, presentations and parent notes, are available to parents on request. Schools are encouraged to promote CyberSafe practices through the inclusion of resource guides with the school newsletter.

PARENT INFORMATION SHEETS

CYBER-SAFETY
The Diocesan School network provides students and teachers with access to the internet for learning, teaching and administration activities. It is acknowledged that along with the many benefits that access to the Internet provides that parents and students need to be aware of those aspects of the Internet which can be a danger to the safety and well-being of all.

The following Information Sheets are suitable for circulation to parents through the school newsletter:

1.	Supervising Children On-Line	NetAlert Bulletin	02339
2.	Safety Tips for Kids and Teens	NetAlert Bulletin	02321
3.	Cyber-bullying	NetAlert Bulletin	02315
4.	Cyber Stalking	NetAlert Bulletin	02317
5.	Mobile Internet Enabled Devices	NetAlert Bulletin	02349
6.	Internet Safety Contacts	NetAlert Bulletin	02329
7.	Stay Safe in Chat Rooms	NetAlert Bulletin	02343
8.	Paedophiles and On-Line Grooming	NetAlert Bulletin	02333
9.	On-Line Publishing	NetAlert Bulletin	02331
10.	Safe Zones and Labelling Tools	NetAlert Bulletin	02319
11.	Pornography and Inappropriate Content	NetAlert Bulletin	02345

CYBER-SAFETY EDUCATION K-12

The DSS acknowledges that Cyber-safety Education for students is important within the context and demands of 21st Century Learning. There is a need to consider a balanced approach to Cyber-safety in terms of exposing students to a range of explicit and integrated learning activities.

All students will have the opportunity to engage in a range of learning experiences that will be embedded in the school curriculum and also taught directly. It will be possible for students to gain access to high quality on-line educational activities and experiences that support student understanding.

Schools will have to provide evidence that high quality educational experiences around Cyber-safety are made available to students through the Tier One Accreditation and Quality Assurance process.

DBB RECOMMENDED EDUCATIONAL RESOURCES

(BASED ON ACBC FRAMEWORK)

MAIN FOCUS	WEB RESOURCE	CYBERSAFETY CONTENT	RESOURCE MATERIALS	YEAR GROUP
Unwelcome Websites	Netty's World	1. Exploring the net	Parent Guide Available	Year 2, 3, 4
		2. Finding Stuff	Parent Guide Available	Year 3, 4, 5
	Cyberquoll	6. Kids in Cyberspace	Teacher Guide & Student Resources Available	Year 5, 6
Stranger Danger	Hector's World	1. Details, Details	Lesson Plan Available	K, 1, 2
		2. Welcome to the carnival	Lesson Plan Available	K, 1, 2
		3. It's a Serious Game	Lesson Plan Available	K, 1, 2
		4. The Info Gang	Lesson Plan Available	K, 1, 2
		5. Heroes	Lesson Plan Available	K, 1, 2
	Netty's World	4. Putting work on the net	Parent Guide Available	Year 3, 4, 5, 6
		5. Making Friends on the net	Parent Guide Available	Year 3, 4, 5, 6
	CyberQuoll	4. Sharing Web content	Teacher Guide & Student Resources Available	Year 3, 4, 5, 6
	Cybersmart Detectives	Identity Hiding on-line	Teacher Guide Available	Year 5, 6, 7
	Netty's World	My Plan: Personalised Safety Action Plan	Parent Guide Available	Year 7, 8, 9
		Quiz: Don't Diss Me	Parent Guide Available	Year 7, 8, 9
	Cybernetrix	Simulated Chat Room	Teacher Guide & Student Resources Available	Year 7, 8, 9
	Wise Up To IT	Jeremy's Friend	Teacher Guidelines Available	Year 7, 8, 9
Cyber Bullying	Cyberquoll	3. Making Waves	Teacher Guide & Student Resources Available	Year 4, 5, 6
	Cybernetrix	Mobile Phone	Teacher Guide & Student Resources Available	Year 6, 7, 8
		Quiz: keeping it real on-line	Teacher Guide & Student Resources Available	Year 6, 7, 8
	Wise Up To It	Stalking Sarah	Teacher Guidelines Available	Year 7, 8, 9, 10
		Lauren's Ordeal	Teacher Guidelines Available	Year 7, 8, 9, 10
Financial Exploitation	Netty's World	3. Using Smart Phones	Parent Guide Available	Year 4, 5, 6
	Cyberquoll	5. Trying it on	Teacher Guide & Student Resources Available	Year 5, 6, 7
	Cybernetrix	Quiz: Danger, Spam and Scams	Teacher Guide & Student Resources Available	Year 7, 8, 9
		Mobile Phone Interaction	Teacher Guide & Student Resources Available	Year 7, 8, 9
	Wise Up To It	What the ?	Teacher Guidelines Available	Year 7, 8, 9
Unlawful Use	Netty's World	2. Getting things off the net	Parent Guide Available	Year 3, 4, 5, 6

CYBER SAFETY INCIDENT / BREACH IS DISCOVERED

UNWELCOME WEBSITES | CYBERBULLYING | STRANGER DANGER | ILLEGAL ACTIVITY | FINANCIAL EXPLOITATION

- **Record what is known about the incident using the Cyber Safety Incident Sheet after the student(s) is/are interviewed.**

- **Inform the Assistant Principal / Deputy Principal as soon as practicable. Cyber Safety Incident Sheet to be passed on.**

- **Assistant Principal / Deputy Principal notifies the Principal that a breach has occurred.**

UNWELCOME WEBSITES

- **SINA Administrator** adds the offending website to the school filter list.
- **SINA Administrator** may utilise the School Traffic URL interface to determine if other users have accessed the site. This information is communicated to the Assistant Principal/Deputy Principal.
- **SINA Administrator** may utilise the **School Traffic Log On** Search interface to determine if the offending user has accessed or attempted to access other inappropriate websites. This information is communicated to the **Assistant Principal/Deputy Principal**.
- **Assistant Principal / Deputy Principal and Principal** decide on consequences that reflect the School AUA or Student Code of Conduct.

FINANCIAL EXPLOITATION

- **SINA Administrator** assists in the retrieval of evidence that Illegal Activity has taken place. This may include screen dumps of conversations and emails. This may include gaining support from the **CeNet** helpdesk. This may also involve the searching of connected devices.
- **SINA Administrator** assists in the retrieval of evidence that Financial Exploitation has taken place.
- **Assistant Principal / Deputy Principal and Principal** may contact the Police for further assistance.

STRANGER DANGER

- **SINA Administrator** assists in the retrieval of evidence that Stranger Danger has taken place. This may include screen dumps of conversations and emails. This may include gaining support from the CeNet helpdesk.
- **Assistant Principal / Deputy Principal and Principal** may contact the Police for further assistance.

CYBER BULLYING

- **SINA Administrator** assists in the retrieval of evidence that Cyber Bullying has taken place. This may include screen dumps of conversations and emails. This may include gaining support from the CeNet helpdesk.
- **Assistant Principal / Deputy Principal and Principal** decide on consequences that reflect the School AUA or the School's Anti-Bullying Policy and procedures.

ILLEGAL ACTIVITY

- **SINA Administrator** assists in the retrieval of evidence that Illegal Activity has taken place. This may include screen dumps of conversations and emails. This may include gaining support from the **CeNet** helpdesk. This may also involve the searching of connected devices.

SAMPLES OF SCHOOL-BASED INCIDENT RECORDING

CYBER SAFETY INCIDENT REPORT	
Name of Teacher: **Name(s) of Students:** **Date of Incident:**	
❑ **Unwelcome Websites** ❑ **Cyber Bullying** ❑ **Stranger Danger** ❑ **Illegal Activity** ❑ **Financial Exploitation**	**Description of Incident:**
❑ **SINA Administrator Informed** ❑ **AP / Deputy Informed** ❑ **Principal Informed**	**Follow Up:**

CYBER SAFETY INCIDENT REPORT	
Name of Teacher: **Name(s) of Students:** **Date of Incident:**	
❑ **Unwelcome Websites** ❑ **Cyber Bullying** ❑ **Stranger Danger** ❑ **Illegal Activity** ❑ **Financial Exploitation**	**Description of Incident:**
❑ **SINA Administrator Informed** ❑ **AP / Deputy Informed** ❑ **Principal Informed**	**Follow Up:**

RELATED POLICIES

The DBB Cyber-safety Guidelines draw on a range of existing DSS policies that include, but are not limited to the following:

- Pastoral Care Policy
- Anti-Bullying Policy
- Anti-Harassment Policy
- Complaints Handling Policy and Procedures
- Creating Safe Supportive School Environments-Child Protection Policy
- Internet and Network Services Policy
- OHS Policy
- Student Discipline Policy