YOUNG PEOPLE AND TECHNOLOGY

A review of the current literature (2ⁿᵈ edition)

Prepared by

Professor Helen McGrath
Adjunct Professor
School of Education
RMIT University

for

The Alannah and Madeline Foundation

Contact

Jackie Van Vugt
General Manager, CyberSafety
The Alannah and Madeline Foundation
jackie.vanvugt@amf.org.au

YOUNG PEOPLE AND TECHNOLOGY
Note: The term 'young people' is used in this literature review to identify children and adolescents aged from 5 to 18 years of age.

New technologies have both potential and challenges.
Diamanduros et al. (2008) have noted that 'never before, in the history of education, have more students had access to so many resources' (p.693) and most of these resources derive from new electronic communication technologies that continue to evolve ever more rapidly. Belsey (2008) points out that instant messaging is growing at a rate 30% faster than email did at its inception. This wonderful range of new technologies offers enormous educational potential for both teachers and students but also some serious challenges. The overall challenge for schools is embracing these new technologies as positive tools for teaching, learning and building relationships whilst at the same time identifying and addressing the safety risks attached to their use. Students are starting to develop a moral compass with which to navigate their way through cyberspace (Bauman, 2007) but have limited experience in assessing risk and predicting and weighing up the potential consequences of their behavioural choices (Berson and Berson, 2005).

Do young people use technology in different ways to most adults and value it more?
Young people appear to use technology in ways that are different to most of their teachers and parents. Adults (depending on their age) typically use Information and Communication Technologies (ICTs) as functional tools that are used for practical or business purposes. Parents and teachers see technology as being most beneficial for accessing new knowledge and learning.

Young people on the other hand see technologies (and especially the internet) as a vital part of their social life and the building of their identity. Mobile phones seem to be the key to young people's social lives, especially in Australia (ACMA, 2007). They have become status items that reflect the emerging identities of young people (Belsey, 2008) who personalise them (e.g. by selecting colour, size, covers and ringtones) and compete to have the newest phone with the widest capabilities. A study by the McCrindle research group (Hale, 2009; McCrindle, n.d.), indicated that whereas the milestones of previous generations included leaving school, getting a job or moving out of home, the most significant milestones towards adulthood are now acquiring a mobile phone and joining online social networking sites.

Bauman (2007) argues that young people place a high value on technology because it is one of few areas where their knowledge and skills exceed most of the adults with whom they interact. However, although this may be true of mobile phone technology, it may not be accurate when applied to internet usage. One Canadian study (IPSOS, 2008) found that young people (at least in Canada) may not in fact be sophisticated users of technology, with only 28% of young people aged 12-17 rating themselves as very skilled or expert in the use of the internet, 48% rating themselves as fairly skilled, and 24% rating themselves as not being skilled. However another Canadian study (IPSOS, 2008) found that young people aged 13-17 are far more aware than adults of online social networks or communities such as Windows Live Space, YouTube, Facebook, and MySpace and this is probably so in Australia as well.

Belsey (2008) has described young people as always 'on' i.e., continuously connected to technology of one kind or another. However the Canadian IPSOS study (2008) has challenged this stereotype as well. These researchers found that young people in Canada aged 12-17 were not online as much as the stereotype suggests, with the average time spent online being only 13 hours per week, compared to an average of 19 hours per week for adults.

One UK study of young people aged 5-16 years (ChildWise, 2009) found that the average number of hours per week spent online was only 10 hours and only a minority of teenagers (37%) agreed that using the internet is an important part of their day (compared to 51% of adults).

According to ACMA (2007) Australian children (spend an average of one hour and 17 minutes per day using the internet, which amounts to 9 hours per week. This includes (each day):

- 49 minutes of internet activities such as messaging, visiting social websites and emailing;
- 15 minutes playing games online against other players; and
- 13 minutes doing homework on the computer and/or internet.

Most researchers agree that the internet is perceived by young people as a normal and healthy form of communication that helps them to stay connected to their peer group, often in 'real time' through the instantaneous mode of instant messaging (IM) (Belsey, 2008). The Canadian ISPOS study identified that: 61% of the young people they surveyed (aged 12-17 years) reported that the internet is important to their social life (61%), and 88% reported participating in an online social activity (compared to 70% of adults), with 59% reporting that they visited online social networks or communities from a few times a week to daily. This social connection is very important to their social wellbeing (Berson, 2003; Campbell, 2005; Gross, Juvonen and Gable, 2002).

The Generation Gap: Are parents unaware of the risks?
Huffaker and Calvert (2005) describe a 'generation technology gap' which is maintained by 'netspeak', a continually evolving language that is rarely used in other aspects of the lives of young people and which involves abbreviations, acronyms, variations on words, emoticons (icons which indicate the communicator's feelings) or avatars (graphical icons and online personas that represent the user). However a study by Microsoft and IPSOS (2007) identified a surprisingly small gap between how parents think their children are using technology and the reality of the risky activities that many of them are participating in. The ACMA study (2007) of Australian families found that most parents (97%) use the internet themselves and are comfortable doing so. However they may not be using more complex features such as blogs, video-sharing websites, chat rooms and social networking sites.

Cross, Shaw, Hearn, Epstein, Monks, Lester, and Thomas (2009), in their Australian study of students in year 4 through to year 8, identified that 22% of them reported that there were rules at home about mobile phone use and 49% reported that there were rules at home about internet usage. The ACMA study (2007) found that most parents trusted their child's judgement about the internet and, at least some of the time, leave it up to him/her to choose what is done on the internet (83%). However the majority of parents (81%) also reported that they make sure or check that certain websites or online activities are OK for their child at least some of the time. Of that number, 62% do so all the time or most of the time. The majority of parents (82%) also keep an eye on the screen when their child is using the internet at least some of the time. Many parents (60%) talk with their child about what s/he does on the internet at other people's houses. Parental checking of and restrictions on internet activity is more common overall for 8–15 year olds (81%) than for 16 year olds (69%) or 17 year olds (51%). Parents reported that certain factors made it difficult for them to monitor and manage their children's internet and mobile phone use. These included:

- Not always being able to keep an eye on the screen or what their child is doing.
- The amount of time children spend on these activities and the all-consuming nature of many of them.
- Children's resistance to being given time limits.

- The difficulty of preventing exposure to inappropriate content.
- Mobile phones and computers being used behind closed doors or outside the house. This is a particular difficulty with 3G mobile phones which can also access email and internet and with notebook computers using wireless technology.
- Children's ability to control their own use of the internet, email and mobile phones via phone locks, access passwords and being able to hide their web browsing history.
- The difficulty that parents experience in keeping pace with technological advances, especially in relation to the internet.

This last point suggests that many parents may be unfamiliar with some of the more complex features of the internet, such as social networking sites and virtual reality sites, and hence the risky aspects of them.

WHAT IS CYBERSAFETY?

The Alannah and Madeline Foundation's cybersafety framework for schools initiative is designed to support schools to enhance their practices in relation to developing and sustaining an overall *safe school* in which risk and harm from all sources, including cyber-risks (i.e., cyber-exploitation, cyber-attacks, cyberbullying and unacceptable or unethical use of technology) is minimised and technologies are used in a safe, resourceful and responsible way. This is part of a larger plan for community change.

> Cybersafety refers to the safe and responsible use of the internet and ICT equipment/devices, including mobile phones (NetSafe NZ, n.d.).

> ACMA's cybersafety activities aim to give children, their parents/carers and teachers, sound advice on how best to manage online risks, so their experiences are safe and positive (ACMA, 2007).

> The use of a set of precautionary policies, practices and actions taken by individuals, schools and communities to prevent harm to users of technologies within the school community, and to promote smart, safe and responsible behaviour (AMF Cybersafety and Wellbeing Initiative, 2009).

Cyber-risks

Cyber-risks are potential threats to the wellbeing of users of technology within the school community and include:

Cyber-exploitation
The use of the internet to manipulate others for one's own self-serving or dishonest ends (mainly financial and sexual).

Cyber-attack
A single or 'one-off' act of aggression, denigration or nastiness against a specific student via technology. Cyber-attacks include, for example, cyber-threats, cyber-insults and cyber-humiliation.

Cyberbullying
A repeated or sustained pattern of intentional cyber-attacks that causes distress and is directed against a specific student or group. Cyberbullying can also be a multi-faceted or multi-step campaign of humiliation or hostility that causes distress and is directed against a specific student or group.

Unacceptable or inappropriate use of technology
This includes user behaviour which is offensive, self-risking, illegal, unethical or uncritical. Examples include: downloading/uploading/transmission of highly personal

content or offensive material; plagiarism; copyright infringement; uncritical use of the internet as a source of information.

Not all online activities of young people are risky and there are a number of other terms that should be clearly differentiated. These include:

- *Cyber-jokes and cyber-teasing*: In their investigation of cyberbullying with students aged 10-18 years, Vandebosch and van Cleemput (2008) identified that students perceived there was a difference between a cyber-attack or cyberbullying and cyber-jokes, cyber-teasing and cyber-fighting. Cyber-jokes and Cyber-teasing were described as communications that are not *intended* to cause negative feeling and are just meant to be funny. The respondents acknowledged, however, that there might be a difference between the way things were intended and the way things were perceived. What some students considered an innocent joke might be considered an aggressive attack by the person on the receiving end (or even the other way around). The respondents also reported that the decision about whether or not a communication was a joke or a humiliating cyber-attack or part of a cyberbullying pattern was usually made on the basis of the relationship between the parties involved.

- *Cyber-fighting:* This was described as mutual online nastiness or cyber-attacks, often starting as part of, or after, an argument between two or more people who may be friends or former friends and who are considered to be 'equals'. It is similar to the notion of mutual conflict which is also differentiated from offline bullying (McGrath, 2007).

CYBERSAFETY: LEGAL ISSUES
All kinds of cyber-risks have legal implications. Reasonably clear evidence is usually available about an individual's behaviour online and their use of a mobile phone. Despite a user's attempts to remain anonymous, law enforcement has the authority, skills and tools to identify the 'digital footprints' that always remain. Whether or not they use these powers is determined by a range of factors such as the type of behaviour, its severity and whether or not it involves criminal action. Several Australian private investigation firms have also added a 'technological investigation' arm to their businesses, tracking down and finding evidence for cyber-attacks and cyberbullying.

Cybersafety reflects legal issues and implications such as:
- the balance between freedom of speech, the right to privacy and cybersafety;
- criminal charges against users;
- discrimination and racial vilification;
- civil claims against users;
- legislation controlling the behaviour of ISPs (Internet Service Providers); and
- the responsibility and rights of the school in responding to a cyber-attack or cyberbullying that occurs outside school hours and off the school premises.

The balance between freedom of speech, the right to privacy and cybersafety
There can be a conflict between cybersafety and freedom of speech and the right to privacy (Shariff, 2006, 2009). For example it can be argued that a person has the right to post a comment online which outlines their views about someone's character or a comment they have made. At the same time it can also be argued that the person who is being commented on has the right not to be harmed by the comments of another that might damage their reputation. Having a moderator in a chat room who can block a user's access because they insulted someone or used a hostile tone could also be seen as a violation of a person's right to free speech and privacy. Nobody has that role for telephone conversations and most people would be horrified to think that a moderator could terminate a phone call under

similar conditions. However, because an online communication is usually more public, there may be more harm caused to the recipient.

Criminal action against users
Bullying and cyberbullying can be addressed by a range of criminal legislation which focus on the both the specific behaviours and/or the technology involved. These include stalking, threats to kill or harm, malicious damage (e.g., by sending a virus), 'acting in concert' in the above intentions and racial vilification (Adams, 2007; Nicholson, 2006).

E-crime is a new term that covers criminal offences committed when a computer or other electronic communication devices (e.g., mobile phones):
- are used in committing the offence;
- are targeted in an offence; or
- act as a storage device in an offence.

More details can be obtained from the website of Department of Education and Children's Services, South Australia (http://www.decs.sa.gov.au/docs/documents/1/CyberBullyingECrimeProtec.pdf.

The following are some examples of Australian e-crime offences and penalties:

> *Impersonation*
> A student dishonestly obtains someone's email address and access information and sends an offensive email to everyone in that person's email address book.
> The offence: Unlawful operation of computer system.
> The maximum penalty: Imprisonment for 6 months or $2,500.

> *Child pornography*
> Uploading a photograph of someone under-age who is naked (e.g., whilst he/she is changing for sport in a locker room and isn't aware of being photographed and then transmitting it to others).
> OR (if under-age)
> Taking a photo of oneself naked and uploading it to a website.
> The offence: Production or dissemination of child pornography.
> The maximum penalty: Imprisonment for 10 years.

> *Hate website*
> A group of students create a racially focused hate website about their classmates.
> The offence: Racial vilification.
> The maximum penalty: $5,000, or imprisonment for 3 years, or both.

> *Cyber-attack*
> A threat to hurt someone is sent via text message or email.
> The offence: Using internet or mobile phone carriers to make a threat.
> Maximum penalty: Imprisonment for 7 years.

> A humiliating and untrue story about someone is posted online and others are invited to comment on it.
> The offence: Using internet or mobile phone carriers to menace, harass or cause offence.
> The maximum penalty: Imprisonment for 3 years.

The US Congress passed a law (in 2006) which made it a federal crime to 'annoy, abuse, threaten or harass' another person via the internet. An additional 36 states have followed

this path, but this law only applies to people over 18 years of age. However McKenna (2007) has suggested that there is some reluctance on the part of law enforcement to prosecute this kind of 'soft crime'.

Discrimination

Claims can be made to the Equal Opportunity Office against people who behave online or via mobile phone in ways that discriminate on the basis of race, gender, sexual orientation etc. In some cases claims may also be made against the ISP that allowed it.

Civil claims against users and ISPs

There are several kinds of civil claims that can be made in relation to a cyber-attack or cyberbullying and, in some cases, inappropriate use.

> *Compensation claims* can be made by a student against a specific teacher, a school or a school system for harm suffered as a result of failure to exercise their duty of care through *negligence* (i.e., failure to take reasonable care) or by ignoring bullying behaviour (including cyberbullying) which has been reported or brought to the attention of a school in other ways or not acting in a way which would prevent foreseeable outcomes (Best, 2007; Nicholson, 2006). Such claims can be made shortly after bullying or cyberbullying occurs or many years later. It is expected that a school's duty of care includes planning and implementing policy and programs to actively eliminate bullying, being vigilant in identifying potential bullying behaviour and breaches of cybersafety and students who engage in it, and responding to reports/complaints of bullying appropriately (Best, 2007).

> A *defamation/libel claim* can be made against a student or a several students or against a school or school system. It is less that such a claim made by a student would be successful as they do not have an income that would be affected by reputation damage. However in some cases a claim can be made by members of a students' family if the cyberbullying against a student included the posting or sending of messages that told lies about or publicly humiliated those family members either by words or images. In 2007 The UK Association of Teachers and Lecturers (ATL) stated that, in support of teachers who had been libelled or humiliated online, they would be prepared to take legal action against the publishers of websites such as RateMyTeachers.co.uk and YouTube, who have allowed students to post abusive and false information about them and humiliating video-clips and photographs of them taken at school using mobile phones (Frean, 2007). Teachers have been maliciously attacked and humiliated in a range of ways. For example, one student posted a photograph of a teacher's face which had been superimposed on someone else's naked body. Another posted lies about a teacher's sex life. Some students have taken (with a mobile phone) and posted photographs of teachers' cleavages, naked flesh or underwear (taken as they bend over). The organisation noted that such postings could adversely affect teachers' job selection and promotion opportunities and be held to be defamatory or libelous. Although both RateMyTeachers and MyTube have clear guidelines for users about unacceptable comments, language and postings, the ATL questioned the efficiency with which both operators policed their sites (Frean, 2007).

Legislation controlling the behaviour of ISPs (Internet Service Providers)

Although Internet Service Providers will generally respond to complaints it may take them some time and their response may not be satisfactory. An 'internet real-name system' was introduced in South Korea in 2005. This law forces online portals, news websites, video sharing sites, email systems, blogs and chat rooms to keep a record of the identity and contact details of people who apply for an account and who post content. They are required

to disclose their contact details if someone wants to sue them for libel or infringement of privacy. The system has been criticised on several grounds; for example, on the grounds that prohibiting anonymity of expression is a violation of the right to free speech. The 'real name' system requires that users submit their national ID and the national ID database is used to verify real names. It has been argued that this also infringes people's right to privacy (Kim, 2005).

The responsibility and rights of the school in responding to a cyber-attack or cyberbullying that occurs outside school hours and off the school premises

Many research studies (e.g., Cross, Shaw, Hearn, Epstein, Monks, Lester, and Thomas, 2009; Smith et al., 2008) suggest that cyberbullying occurs more outside the school and in non-school hours than at school during school times. Schools are sometimes reluctant to become involved when cyberbullying occurs outside of school hours, off the school campus, and without the use of school computers. However as Spears et al. (2008) have explained ' …what has occurred within relationships whilst at school, can be continued on-line at home or on the weekend, and any fallout in those relationships during the time on-line recurs back at school the next day or after the weekend. This *cyclical, sequential* nature of the behaviours suggests that the jurisdiction between home and school will need to be rethought, as well as previous understandings of bullying as being discrete, different types of behaviour (physical, verbal, social, psychological; indirect, relational) associated with gender or place or time' (p.16). Ford (2007) argues that the relationship of teacher and student does not necessarily start and end with a student's arrival at and departure from school, and a particular duty of care may arise because of that pre-existing relationship.

There is a growing trend for schools both in Australia and internationally to take some level of responsibility for the management of situations that involve a cyber-attack or cyberbullying that occurs outside school hours and involves students from the school. For example T*he Education and Inspections Act 2006* (EIA 2006) in the UK includes legal powers that enable principal-level staff to regulate the conduct of students when they are off-site and provides a defence in relation to the confiscation of mobile phones and other items at school.

Willard (2007a, 2007b) believes that a number of successful law suits in the USA (brought by parents against schools who had taken action against their children who had cyberbullied other students offsite) have helped to clarify the rights and responsibilities of schools in this regard and have encouraged legislators to provide schools with stronger legal rights. Many schools in the USA now have legal rights to intervene in incidents of cyberbullying, including those initiated off the school campus, if there is evidence that the incident resulted or could result in a substantial disruption of the school environment (Hinduja and Patchin, n.d.; Shariff, 2009; Willard, 2007a). For example, the Arkansas House Bill HB 1072 (now known as ACT115) states (in part):

> A school policy can extend to electronic acts whether or not the electronic act originated on school property or with school equipment, if the electronic act is directed specifically at students or school personnel and maliciously intended for the purpose of disrupting school and has a high likelihood of succeeding in that purpose (Arkansas House Bill) (Daiamnduros et al., 2008).

Being cyberbullied outside school has the potential to create strong negative emotions in students who are targeted. Feelings of anxiety and embarrassment may negatively affect schoolwork and classroom climate and lead some students to stay away from school (Diamanduros et al., 2008). Feelings of humiliation, shame and anger can lead to potentially dangerous situations for both the victimised student (who may self-harm), those who are suspected of involvement in the cyberbullying (who may be attacked), and other classmates (who may also be attacked) (Willard, 2007a). Thus, what happens between students who

attend the same school, but outside the school, may nonetheless have a very strong impact on what happens at school when it resumes. It makes sense for schools to be informed about what has happened and to have the right to intervene and/or follow up in a timely and effective manner. This may only involve activating the school's behaviour management and welfare procedures when school resumes. However it may also potentially involve at least one member of a school staff being 'on call' during weekends and holiday periods to receive calls from students or parents, to advise as needed and, in some cases, to speak to other parents or contact law enforcement.

Students and parents need to be clearly informed of the school's rights to take action in situations involving behaviors that can have a negative effect on the safety of students, staff, and/or the educational environment. Asking parents and students to sign a contract about this ensures that they understand the consequences of cyberbullying behavior that results in placing student and staff safety at risk and has a negative impact on the educational environment (Diamanduros et al., 2008).

THE USE AND MIS-USE OF SPECIFIC TECHNOLOGIES

YOUNG PEOPLE AND MOBILE PHONES
Students can use mobile phones for phone calls and text messaging (involving text, picture and video). The ACMA (2007) study of Australian families identified that:

- 54% of Australian children aged 8-17 have their own mobile phone.
- Mobile phone use increases with age—from 16% of eight year olds up to 90% of 17 year olds. There is a marked increase in usage at age 12 (57%).
- Use of mobile phones to take photos and listen to music increases from 14 years of age onwards.
- Girls use mobile phones more (63% overall) than boys (44%).
- Girls also use text/picture messaging more (45% girls, 26% boys), make and receive phone calls more (43% girls and 26% boys) and take photos more (30% girls and 15% boys).
- Only 18% of children and young people use 3G mobile phones which have internet access and video content.

Positive uses of mobile phones
Examples include:
- Facilitates social communication and the development of relationships.
- Enhances personal security.
- Photographs taken with a mobile phone can be incorporated into aspects of schoolwork.
- Provides opportunities for the development of values and skills associated with digital citizenship.
- Fosters the development of technological skills and media literacy.

Cyber-exploitation via mobile phone
Examples include:
- Students can be exploited by unscrupulous salespeople who try to sell them expensive and possibly disadvantageous mobile phone plans.
- Services (e.g., Valentine's Day greetings marketed by Telstra) are often marketed via text messages.
- A boy can entice a girl (with whom he may currently have a romantic relationship) to take sexual photos of herself using the camera in her mobile phone and transmit them via the phone. The boy (perhaps after a break up) may then share the

photographs with others via phone (or upload them onto a website) without the consent of the girl who appears in the photographs.

Cyber-attack via mobile phone (a single or 'one-off' cyber-threat, cyber-insult, cyber-humiliation, etc.)

Examples include:
- A threat to harm another student is transmitted by phone call or text message.
- A one-off insult is sent via text message or phone call, e.g., a nasty, ridiculing, denigrating, homophobic, sexist or racist comment; a derogatory name is used (e.g., slut, fag, etc.).
- A single hang-up phone call is made or a call is made or text message sent in the middle of the night.
- Someone's mobile phone is hidden or taken.
- A single text message is sent to others that contains rumours, private information or vicious comments about one student.
- A single unflattering, humiliating or incriminating photograph is sent as a message without the person's consent.
- Someone's mobile phone is 'borrowed' and a student impersonates the owner and sends a text message that provokes, insults or threatens another person or makes a sexual overture to them.
- Someone's text message containing private information or image is sent to others without consent.
- An unwanted offensive image is sent via text message to someone.

Cyberbullying via mobile phone

Bullying may involve repeated threats, attacks, humiliations or insults of the same kind or there may be a variety of attacks using mobile phones in different ways. Examples include:

- A group of students make a plan to collaboratively make fifteen or more hang-up calls to another student's mobile phone every day for a week. Making calls in this way to a student's mobile phone is a more 'effective' method than making prank calls to the student's home where the phone could be picked up by family members.

- The putting together of a multi-step, complex and sustained campaign of humiliation or insult (e.g., by 'setting up' a situation to humiliate a specific student such as by starting a fight with them, getting them to reveal a secret about themselves or having someone pretend to ask them out or like them), video-recording the event on a mobile phone and then sending it to others via mobile phone (or posting it online) without their consent.

Unacceptable or inappropriate use of mobile phones (i.e., usage which is offensive, self-risking, illegal, unethical or uncritical)

Examples include:
- Forwarding another student's text messages or images on to others (e.g., all recipients in an extended peer contact list) without permission.
- A student uses a mobile phone to take photos or record situations of a crude, violent or sexual nature and then transmits them to others via mobile phone or uploads them onto a website.
- A student uses their phone to take sexual photos of themselves (with no enticement from another to do so) and transmits it to others or uploads it.
- A student uses a 3G phone (which has internet capacity) to download unacceptable or offensive material or illegally download music or video files.

YOUNG PEOPLE AND THE INTERNET
The ACMA Study (2007) identified that almost all Australian children (93%) use the internet at home, at school, or in both settings; and that secondary school aged children use the internet more than primary school aged children. Most of the time (76%) spent by children and young people on the internet is either at home and alone or by themselves but with others in the room (ACMA, 2007). More girls than boys use the internet for music (66%), viewing images (76%) and communicating with others, for example: by emailing (72%); chatting (66%); visiting user-generated video-sharing websites such as YouTube (48%); and working on their own material to post on the internet (31%). More boys than girls use the internet to play games against others online (39%), use shopping or auction websites (20%), and watch downloaded television shows, clips and cartoons (18%).

Two in five young Australians aged 8-17 (42%) reported having their own material on the internet in some form (ACMA, 2007), with 80% of 14–17 year old girls and 65% of 14–17 year old boys having some form of web authorship.

YOUNG PEOPLE AND EMAIL
Email enables text communication and the capacity to attach files and photographs. Using email is a cheaper way to communicate than using phone-based text messages, and students often have more than one email address. Students who are sophisticated in the use of technology are able to send emails in a way which hides the identity of the sender (although this can be deciphered by experts).

Positive uses of email
- Writing to email pen-pals can be incorporated into the curriculum.
- Enables collaboration on a project with other group members.
- Facilitates social communication and the development of relationships.
- Enables staying in touch when classmates change schools or location.
- Enables students to report bullying or speak to a teacher about other matters in a confidential way.
- Provides opportunities for the development of values and skills associated with digital citizenship.
- Fosters the development of technological skills and media literacy.

Cyber-exploitation via email
Students can be exploited through emails that are sent to them offering special deals, free memberships, gaming or gambling opportunities or phony prizes. They may be encouraged to pay for these by giving details of their own debit card or a parent's credit or debit card. 'Phishing' is also common, i.e., students are fooled into providing their personal or financial details.

Cyber-attack via email (a single or 'one-off' cyber-threat, cyber-insult, cyber-humiliation, etc.)
Most of the threats, insults and attacks that can be delivered via phone calls or text messages can also be delivered via email. Humiliating photos (or a video-recording from a mobile phone) can be attached and sent via email. A student's email address can be dishonestly obtained and used by another student to impersonate them (as outlined above). A student may try to get another student into trouble by sending a provocative or threatening message which elicits a counter-attack. This counter-attack is then complained about to the school or other authority as if it were an initial and unprovoked attack. A student can send a virus to another student by email in an attempt to damage his/her computer or erase their hard drive. Someone's email message or attachment containing private information or images is sent to others without consent.

Cyberbullying via email
This is a pattern of repeated and/or sustained threats, attacks, insults or impersonations via email text and/or attachments as outlined under the section on mobile phones.

Unacceptable or inappropriate use of email (i.e., usage which is offensive, self-risking, illegal, unethical or uncritical)
Email is used to transmit unacceptable or offensive material to others. Email messages can be copied without the permission of the sender and forwarded to other people for whom they were not intended and/or who were not on the sender's contact list.

YOUNG PEOPLE AND INSTANT MESSAGING (IM)
Instant messaging enables real-time very fast communication on the internet between two or more people who communicate using typed text. It could be described as instant emailing. IMs can only be sent to and from subscribers who have listed each other as contacts. Users can choose those with whom they want to chat and those they want to exclude. Users are alerted when somebody on their personal list is online. Instant messaging programs are usually a one-to-one communication medium, but some programs allow many people to chat to each other at the same time, much like a private chat room (NetAlert, n.d.). Using instant messaging is cheaper than making mobile phone calls or sending text messages and faster than email. Three commonly used IM programs are:

- Windows Live Messenger (formerly called MSN Messenger), (messenger.ninemsn.com.au)
- Yahoo Messenger (au.messenger.yahoo.com)
- AOL Instant Messenger (www.aim.com)

Skype is a phone and video-phone software program that also has instant messaging capability. If webcams are used by both communicators then video phone calls can also be made during which IM can also be used and files can be attached.

In the IPSOS Canadian study (2008) 74% of young people aged 13-17 indicated that they had used instant messaging to communicate with friends or family members. Instant messaging was used by 74% of this group to communicate with friends or family members. Bauman (2007), and Grinter and Palen (2002) have suggested that instant messaging is especially popular with students aged 11-15 years, as they have a strong interest in socialising but lack access to the independent transport that would make face-to-face social activity outside school easier.

Positive uses of instant messaging
- Enables collaboration on a project with other group members.
- Facilitates social communication and the development of relationships.
- Enables staying in touch when classmates change schools or location.
- Provides opportunities for the development of values and skills associated with digital citizenship.

Cyber-attack via instant messaging (a single or 'one-off cyber-threat, cyber-insult, cyber-humiliation, etc.)
Most of the threats, insults and attacks that can be delivered via phone call, text message or email can also be delivered via IM. Screen names can conceal a student's identity. It is possible to break into someone's MSN account and delete their contact list.

Cyberbullying via instant messaging
IM can be used as part of a bullying pattern which may also include other types of cyber-attacks. IM can also be used in many different ways to bully another. Students can socially exclude one student by repeatedly removing them from access lists. One student or a group

of students may encourage a specific student to regularly disclose personal information which is then sent to many others (who are not on his/her contact list) without permission. Large numbers of winks or buzzers (annoying animated icons with sound) may be sent repeatedly to someone.

Unacceptable or inappropriate use of instant messaging (i.e., usage which is offensive, self-risking, illegal, unethical or uncritical)
An IM message can be copied without the consent of the sender and forwarded to other people who were not intended recipients and/or were not on the sender's contact list.

YOUNG PEOPLE AND CHAT ROOMS

A chat room is an internet site where people with a shared interest can 'meet' and communicate by typing messages to each other on their computer in real-time. Text can provide links to Web pages. Messages that are typed in by a user appear instantly to everybody who is in that chat room (NetAlert, n.d.). Some sites are open to anyone and have a specific focus (e.g., movies, rock groups, antique aircraft, British history, old coins, Australian birds) and most of the participants have never met face-to-face. Others have only restricted access and are by invitation only but having many contacts on their buddy list may increase young people's sense of popularity and connection. Some chat rooms are focused on making friends and developing relationships. People don't always have to verify who they are before they enter a chat room and screen names can conceal a student's identity. Some chat rooms are moderated by someone who is keeping an eye on the content, language and tone of the messages but most are not. It has been argued, and noted above, that such monitoring is a violation of privacy similar to having someone monitoring your phone calls.

A study of 40,000 students in the US aged 14-15 years (Beebe, Asche, Harrison, and Quinlan, 2004) found that almost half of students with home internet facilities accessed chat rooms; and that those who did so were more likely (than students who did not use chat rooms) to exhibit risky behaviors such as smoking, drug use, early sexual behaviour and running away from home. Bauman (2007) suggests that young people who need support may seek it within a chat room.

Positive uses of chat rooms
- Some interest-based chat rooms can assist learning.
- Enables collaboration on a project with other group members.
- Facilitates social communication and the development of relationships.
- Enables staying in touch when classmates change schools or location.
- Fosters the development of technological skills and media literacy.
- Provides opportunities for the development of values and skills associated with digital citizenship.

Cyber-exploitation via chat rooms
Sexual predators may find chat rooms a simple way to seek potential victims and inappropriate contact can be made by older teenagers or a predatory adult pretending to be a person of the same age. Conversations in unmonitored chat rooms can become sexual in nature, covering topics ranging from sexual 'concerns' to actual cyber-sex activity, which involves text that describes sexual activity in an interactive way (NetSafeKids, n.d.) . Young people who participate in these sexual conversations may be exploited by strangers who are looking for sexual pleasure and/or seeking to establish ongoing relationships which may enable ongoing sexual contact of this kind or further in-person face-to-face exploitation.

Cyber-attack via chat rooms (a single or 'one-off cyber-threat, cyber-insult, cyber-humiliation, etc.)
Most of the threats, insults and attacks that can be delivered via text message, email or IM can also be delivered in a chat room with restricted access. A 'social exclusion' attack can take the form of moving to an invited 'private chat' from which one specific person is excluded or removing a specific student's name from another student's contact list.

Cyberbullying via chat rooms
Bullying can take the form of social exclusion when several students repeatedly (or intermittently but in a sustained way) block one student's access (by removing their names from contact lists) to a limited access chat room that they have formerly participated in. They can be blocked from several different chat rooms with no explanation. Under the guise of friendship, a person or group can repeatedly encourage a specific student to disclose personal information which is then sent to many others via another form of technology (e.g., email) or which is used to ridicule them within the chat room.

Unacceptable or inappropriate use of chat rooms (i.e., usage which is offensive, self-risking, illegal, unethical or uncritical)
Students can access unacceptable or offensive content by asking for sexually explicit images from public chat-room participants (or by responding to offers to provide them) or by visiting a chat room that clearly signals by its name that it contains such content or that it facilitates sexual conversations. They can also access unacceptable content by following the weblinks to such material or sites which may be provided by chat room participants. Students can include their own inappropriate images (e.g., naked photos of themselves) in a chat room and such images may be used by others for commercial gain. Young people can include their own very personal information (e.g., about their sexual interests or their suicidal thinking) in a public chat room. This may be used against them at a later point. Suicidal thinking and self-injurious behaviour may be 'normalised', amplified or encouraged by other chat room participants (Whitlock, Powers and Eckenrode, 2006) either accidentally or intentionally.

YOUNG PEOPLE AND WEBSITES
Students access and create internet websites for many sound reasons for example, to learn, to communicate and to connect. The IPSOS study (2008) found that over half of the Canadian young people in their study aged 13-17 years play online games either against people they know or people completely unknown to them. Sometimes young people use websites in ways that can cause harm to themselves or others.

Positive uses of websites
- Can enhance knowledge and assist learning and research.
- Facilitates social communication and the development of relationships.
- Fosters the development of technological skills and media literacy.
- Supports and develops creativity.
- Provides opportunities for teaching critical thinking.
- Provides opportunities for the development of values and skills associated with digital citizenship.

Cyber-exploitation via websites
Many websites entice students to spend money to access inappropriate images or buy memberships for gaming opportunities or for gambling purposes. They are often asked to pay by providing debit card details and, if they don't have one, to provide a parent's credit or debit card details instead. Some websites are designed to attract young people to provide their personal details and a photo to enable predators to follow up with an email or other form of more personal contact as they attempt to groom them for their own purposes.

Cyber-attack via websites (a single or 'one-off cyber-threat, cyber-insult, cyber-humiliation, etc.)
A student can:
- use their personal website to threaten, attack or insult another student;
- upload a ridiculing comment or other content onto another student's website; or
- register another student to receive unacceptable online content or access to a porn site in order to cause trouble with their family or the school.

Cyberbullying via websites
Bullying via websites involves a pattern of repeated insults or attacks or a multi-step, complex plan which involves setting up and maintaining a website (and advising others how to access it) that causes ongoing and intentional distress to a specific student. This is most commonly done in two ways:

- By impersonating another student (after covertly obtaining their access details) and creating a personal website (text and/or images) in their name which contains false and/or denigrating images and/or information about them (and sometimes about members of their family) that is intended to ridicule and humiliate them. One example: two male students set up such a site in the names of two female classmates that started with text which asserted that they were 'horny, bi-sexual and looking for action'. A week later they downloaded pornographic images of two naked women having sex with each other, altered them so that photographs of the heads of the two female classmates were superimposed and then uploaded them. They then sent bulk emails to their friends giving them the weblink to the site.

- Creating a website that is devoted to damaging the social acceptance and reputation of another student. This can be done by creating a 'hate site' in which classmates or young people in the local district are invited to indicate their shared dislike of a nominated student. It can also be done by creating a polling site which encourages others to vote for which student is, for example, the 'fattest', the 'most slutty', the 'ugliest', the 'most smelly', etc. (after suggesting two or more possible candidates in the category, including the targeted student). It has been suggested that sexual predators who are able to access these sites tend to target the students who are being victimised by contacting them (if they have enough information) and expressing their concern for them as way of 'grooming' them. The names and contact details of the targeted students are often listed on the site.

Unacceptable or inappropriate use of websites (i.e., usage which is offensive, self-risking, illegal, unethical or uncritical)
A student can download violent or pornographic images or text, M-rated/R-rated games, hate speech (e.g., about specific people, races or groups) or the propaganda of cult groups or extremist groups. Students may also post private details or images on their personal websites that may also indirectly cause them harm, for example, by uploading unacceptable or offensive material such as a photograph of him/herself having a sexual encounter. Many students use websites to illegally download or upload music and video. Nearly two-thirds (64%) of young Canadians aged 13-17 reported having downloaded digital music or MP3 files with nearly one-third (30%) reporting that they did so quite often (compared to 7% of adults). Many young people appear to use websites uncritically as an information source or to plagiarise content for assignments.

YOUNG PEOPLE AND BLOGS
The word 'blog' is a merge of the words 'web' and 'log'. Blogs are (mostly) text-based diaries (although some have image uploading capability) which are created and posted online by an individual or organisation. Other people can formally join as members and post their own comments or reply to comments on the current theme. Some blogs are able to be viewed by anyone whilst others are limited to members or selected friends only. Blogs are most

commonly made publicly accessible on the web and they are easier to use than other forms of Computer Mediated Communication as users do not need high levels of expertise. For example they do not need to know HTML or other web programming languages to publish on the internet (Herring et al., 2004). Whereas IM services and some MUDs require users to supply their name, blogs usually do not and that means that users can communicate anonymously.

Blogs are most commonly used as a personal journal or ongoing commentary about oneself (Herring et al., 2004; Huffaker and Calvert, 2005). The ACMA study (2007) identified that 7% of young 8-17 year-old Australians in their study had their own stand-alone blog. Lenhart et al. (2005) reported that 8% of teenagers in the USA read other people's blogs and 19% have their own blog. Huffaker and Calvert (2005) identified that 52% of all blogs are maintained by young people aged 13–19 years. However young people can blur the boundaries between a personal diary and a public blog and hence over-focus on blogs as personal diaries and unthinkingly post personal information that could be exploited or misused by others (Bauman, 2007). For example in a content analysis of 70 blogs of young people aged 13-19 years Huffaker and Calvert (2005) found that:

- 20% provided their real name;
- 44% listed their email address or IM username;
- 49% discussed their romantic relationships; and
- 17% discussed their thoughts about their sexual identity.

Blogs can provide opportunity for self-expression, usually in the form of long, personal, and thoughtful entries (Herring et al., 2004). In a study by Huffaker and Calvert (2005), of the blogs of teenagers, it was apparent that the blogs were mostly perceived by the authors as an extension of their real world, rather than a place where one 'pretends' with many talking about their sexuality, romantic relationships and emotional issues (Huffaker and Calvert, 2005)

Positive uses of blogs
- Huffaker and Calvert (2005) identified that the average blog posting of young people aged 13-19 years was 2,000 words per page, far more than they might usually write in an essay or project. They noted the implications for the potential use of blogs as an educational tool.
- Facilitates social communication and the development of relationships.
- Fosters the development of technological skills and media literacy.
- Supports and develops creativity.
- Enables staying in touch when classmates change schools or location or the family is away from school on an extended trip.
- Provides opportunities for the development of values and skills associated with digital citizenship.

Cyber-exploitation via blogs
The anonymity of blogs, coupled with the degree to which young people appear to speak reasonably openly about themselves, can make blogs appealing places for sexual predators to look for victims.

Cyber-attack via blogs (a single or 'one-off cyber-threat, cyber-insult, cyber-humiliation, etc.)
An insult or attack via a blog usually takes the form of posting another person's comment or secret (true or otherwise) on a blog without their permission or responding to someone's comment in a blog in a nasty or derogatory way.

Cyberbullying via blogs

Bullying may involve repeatedly commenting within someone else's blog in a nasty or derogatory way and/or repeatedly posting another person's comments or personal information/secrets on a blog without their permission.

Unacceptable or inappropriate use of blogs (i.e., usage which is offensive, self-risking, illegal, unethical or uncritical)

A student can inappropriately reveal highly personal information in a blog, for example, about their feelings, sexual concerns or suicidal thinking. Suicidal thinking and self-injurious behaviour may be 'normalised', extended or encouraged by other bloggers (Whitlock, Powers and Eckenrode, 2006).

YOUNG PEOPLE AND ONLINE FORUMS

These are public internet sites where anyone who wants to can contribute to a discussion by leaving a message related to the current topic. It can be likened to a bulletin board. Most users have to register their name and contact information and, in some cases, provide verification of age. However it is possible for someone to register with more than one name and email address. Many forums have moderators who monitor the content, tone and language used and can block people from participating.

Positive uses of online forums
- Online 'limited access' forums can be used within a school context to enable students to comment on new school-based initiatives, for example, suggestions for a new school uniform, etc.
- Can support interest-based learning.
- Provide opportunities for the development of values and skills associated with digital citizenship.
- Foster the development of technological skills and media literacy.

Cyber-exploitation via online forums

Sexual predators may target specific types of forums and try to make contact outside the forum with a specific user.

Cyber-attack via online forums (a single or 'one-off cyber-threat, cyber-insult, cyber-humiliation, etc.)

A student can post another person's comment or secret (true or otherwise) on a forum without their permission. A student can respond to someone's comment in a forum in a nasty or derogatory way.

Cyberbullying via online forums

Bullying involves a patterns repeated attacks as described above.

Unacceptable or inappropriate use of online forums (i.e., usage which is offensive, self-risking, illegal, unethical or uncritical)

A student can make inappropriate or offensive remarks within a forum or inappropriately reveal personal details that enable them to be contacted offline.

YOUNG PEOPLE AND SOCIAL NETWORKING SITES (SNS)

Social networking sites enable individuals to develop a personal profile (using text and/or photographs or images) and to create online friendship networks. People within a network can chat with each other individually or as a group (depending on who is listed as being online at the time) instantly and in real time, share photos and videos and post comments in online forums, blogs or discussion groups (NetAlert, n.d.).Some sites also provide personal web pages for each user. It is possible on some sites to create multiple identities.

Social networking sites commonly used by young people include Bebo, MySpace, Twitter and Facebook. Some sites (e.g., Bebo) are only available to people over a certain age (e.g., 13 years in the case of Bebo). A survey conducted in the UK (Ofcom, 2008) identified that 49% of children and young people aged 8-17 who use the internet have set up their own profile on a social networking site of some kind. However they also found that 27% of the younger children (aged 8-11) reported that they have a profile on one of the major sites for which the minimum age is 13 years and upwards. The minimum age for MySpace is 14 years. Although children and young people must enter their age when they sign in they do not have to verify it and it is very easy to lie about their age. MySpace claims to automatically make the profiles of its 14 and 17-year-old members private. Young Canadians aged 13-17 who are aware of the Windows Live Space social networking site (similar to MySpace) spend an average of 7 hours per week using the site (IPSOS, 2008).

A Xanga is another kind of social networking site. Members do not have access to IM or chat rooms but can have their own web site which consists of a weblog (text), a photoblog (onto which images can be uploaded), a videoblog (video clips), an audioblog, and a social networking profile. Blog-rings or groups can also be created or joined. Users can control other people's access to their sites by using a facility called 'Friends Lock' which allows them to lock out everyone who is not on their list of friends (which can be easily changed). Xanga also has a flagging system that allow users to report sites that contain threatening, offensive or inappropriate content and a 'law enforcement' link to enable users who use inappropriate language or content to be reported. Xanga also includes ratings for each site based on a combination of self-ratings, ratings by other users, and ratings by a moderator. Access to inappropriate and explicit sites is blocked for minors unless they can demonstrate a credit card in their name.

A relatively new social networking site for young people aged 6-12 called SuperClubsPLUS Australia is currently being trialled by the Department of Education and Early Childhood Development (DEECD) with groups of students in Years 3 and 4 across a number of Victorian schools. It is described by DEECD as a safe, actively protected, social learning network for children which provides an engaging learning experience that is centred on ICT literacy and citizenship and allows students to chat and collaborate in a safe environment online. Students can upload media, publish articles, build personalised web pages, run their own clubs, complete projects, join discussion forums, chat with friends, achieve their ICT 'Star Awards', and participate in 'Hot Seats'. The same mediators also stimulate thinking and encourage the children as they grow in online confidence. All students participating are expected to attain their cybersafety star before progressing to further achievements. Qualified teachers with a current Working with Children check act as moderators and monitor students' activities. Many of the activities are specifically designed to engage children in practising strategies to keep themselves safe online.

Positive uses of social networking sites
- Facilitates social communication and the development of relationships.
- Fosters the development of technological skills and media literacy.
- Supports and develops creativity.
- Provides opportunities for the development of values and skills associated with digital citizenship.
- Xanga is primarily a writing site and may have the potential to assist the development of writing skills and support creativity.

Cyber-exploitation via social networking sites
Sexual predators can, on some sites, make contact with young people and attempt to develop a relationship with them that could facilitate contact outside the SNS.

Cyber-attack via social networking sites (a single or 'one-off cyber-threat, cyber-insult, cyber-humiliation, etc.)
A young person can be removed from a contact list that they were part of in order to distress them. An insult or untrue/derogatory comment can be sent or posted about them or a humiliating image of them can be posted. A message or image can be copied without the consent of the sender and forwarded to other people who were not intended recipients and/or were not on the sender's contact list.

Cyberbullying via social networking sites
Bullying involves a pattern of repeated attacks as outlined above. It can also take the form of repeated social exclusion where 'friends' gang up to block one person's access by removing their names from all of their contact lists without explanation. Someone can be repeatedly encouraged to disclose personal information within a social networking site which is then sent to others without consent or used to ridicule them within the site. Multiple 'false' identities can be created within the site who then subject a specific person to ongoing attacks.

Unacceptable or inappropriate use of social networking sites (i.e., usage which is offensive, self-risking, illegal, unethical or uncritical)
A student can upload inappropriate material about, or images of themselves which can be misused (e.g., for commercial gain). A message or image can be copied without the consent of the sender and forwarded to other people who were not intended recipients and/or were not on the sender's contact list.

YOUNG PEOPLE AND VIDEO SHARING SITES
A video sharing site enables people to upload, view and share music, photographs, video blogs and video clips they have created themselves or which have come from another source (e.g., news or sports broadcasts). The best known of these sites is YouTube which prohibits the uploading of videos which defame or which contain commercials, pornography, copyright violations or material encouraging criminal behaviour. Videos that are considered to contain potentially offensive content are available only to registered users over the age of 18. It also offers a personal profile page (referred to as a 'channel page') and enables making friends. Other people can post text comments or make video responses to a video clip. YouTube participants can limit access to their video clip(s) by using the 'friends only' feature or by 'tagging' it (i.e., labelling it and/or naming the creator) in an obscure way. Users can also enable public access without any limits. Individuals can easily subscribe to the videos made by a specific user. When that user creates a new video, the subscriber is notified on their YouTube home page.

Young Canadians aged 13-17 years who report an awareness of YouTube spend an average of 5 hours a week using the site (ISPOS, 2008). Forty-eight percent (46%) of young Australian girls aged 8-17 regularly visit user-generated video-sharing websites such as YouTube (48%).

Positive uses of video sharing sites
- Facilitates social communication and the development of relationships.
- Fosters the development of technological skills and media literacy.
- Supports and develops creativity.
- Provides opportunities for the development of values and skills associated with digital citizenship.

Cyber-exploitation via video sharing sites
Sexual predators can make contact with under-age users as there is no age verification process.

Cyber-attack via video sharing sites (a single or 'one-off cyber-threat, cyber-insult, cyber-humiliation, etc.)

A derogatory comment can be posted about an individual's video clip or video blog. A video or image can be posted which shows a specific student in an unflattering or humiliating light.

Cyberbullying via video sharing sites

A group of students can plan and execute a multi-step campaign which involves setting up a student in a humiliating situation, videorecording it by mobile phone and then posting the video clip on YouTube and inviting derogatory comments from others.

Unacceptable or inappropriate use of video sharing sites (i.e., usage which is offensive, self-risking, illegal, unethical or uncritical)

A student can upload inappropriate video or images of him/herself which can be misused or act as a 'beacon' for a sexual predator. A student can also find ways to access restricted and explicit video clips and images.

YOUNG PEOPLE AND VIRTUAL REALITY SITES

There are many varieties of virtual reality site which have some similarities to a chat rooms but one distinguishing feature is that participants usually do not know each other (Grinter and Palen, 2002). There are three main types of Virtual Reality Sites.

MUDS (Multi-User Dungeons)

MUDS combine elements of chat rooms, 'dragon and dungeon' style role-playing fantasy games (often with a dice). Players interact with each other and the virtual world by typing their commands. Some MUDS are very complex fantasy worlds and participants can create their own identity and have adventures (Suler, 2005). Virtual worlds may be especially appealing to students with low confidence as they are able to recreate themselves.

Massively multi-player online role-playing games (MMPORPGs)

Two MMPORPGS commonly used by young people in Australia are:

- The World of Warcraft (which has a T-rating (Teen 12+) and a moderator.

- Club Penguin, which is a virtual club in which cartoon penguins are the avatars (i.e., represent the players). It is designed for children aged 6-14 years of age and incorporates a moderator who can block access if inappropriate language or behaviour occurs. Players can engage in activities, play games, earn points, develop their own character (avatar) and interact with other 'penguins'. Club Penguin has several built-in safety features such as:
    - A 'Safe Chat' mode which enables users to select their comments from a menu of comments.
    - A filtering system that prevents bad language and does not accept personal information.
    - Moderators who police the game.

Social virtual worlds

The most well-known of these is Second Life, an internet site (restricted to people over 18 years of age) in which users (referred to as 'residents') create their own identities (called avatars) and interact with each other. They can choose to socialise, participate in activities, create and trade virtual property and services or travel throughout the world. A related site called *Teen Second Life* is also available but is restricted to users aged between 13 and 17 years of age who are expected to verify their identification and date of birth. Residents of *Teen Second Life* are transferred to Second Life when they turn 18 and they can take all of their 'assets' with them.

Positive uses of MMPORPGs
- They can assist young people to develop their identity by enabling them to 'try on' different physical and psychological characteristics.
- Facilitates social communication.
- Fosters the development of technological skills and media literacy.
- Supports and develops strategic thinking.
- Provides opportunities for the development of values and skills associated with digital citizenship.

Cyber-attack via MMPORPGs (a single or 'one-off cyber-threat, cyber-insult, cyber-humiliation, etc.)
A student can use their avatar to verbally attack or insult another player's avatar outside the boundaries of the game.

Cyberbullying via MMPORPGs
Bullying usually involves repeated attacks on the same avatar.

CYBERBULLYING
Cyberbullying has been described by Smith et al. (2008) as an important new kind of bullying, with some different characteristics from traditional bullying. Many other writers and researchers (e.g. Campbell, 2005; Li, 2007; Shariff, 2005) have also agreed that cyberbullying can be seen as just another method of bullying and not a separate issue in itself, i.e., that it is 'an old bottle with new wine' (Li, 2007, p.1777), albeit with some different features. Brown, Jackson and Cassidy (2006) note that *the location, actors, language and gestures in face-to-face bullying have evolved and moved into the electronic venue' (p.1).* Li (2007a) has suggested that cyberspace has become another 'playground' for bullying.

A range of electronic communication technologies have now been added to the arsenal of harmful strategies that young people can use to bully others and inflict what Harmon (2004) describes as social cruelty. Spears, Slee, Owens and Johnson (2008) note that (p.19) 'there is now a wealth of opportunity to be creative in one's quest for popularity, and simultaneously, a wealth of ways in which to be persecuted for one's poor judgement'. Cyberbullying can be carried out in many different and sophisticated ways that remove the schoolyard parameters from traditional bullying and expand the problem to the borderless cyberworld (Diamanduros et al., 2008) which is becoming increasingly central to the lives of young people as well as more public (McKenna, 2007). Not being able to access the computer or use your mobile phone means social isolation for young people.

DEFINING CYBERBULLYING
Cyberbullying is a new phenomenon that presents challenges for schools and researchers (Smith et.al., 2008). The first serious challenge for both researchers and the community is to clearly define what cyberbullying is. Many researchers and writers (Baruch, 2005; Belsey, 2008; Patchin and Hinduja, 2006; Kowalski and Limber, 2007; Ybarra and Mitchell, 2004a; Smith, 2006; Smith et al., 2008) believe that the most valid definition of cyberbullying is one that is based on the generally accepted definition of bullying per se. This concept of 'general bullying' is described by Smith et al. (2008) as 'traditional bullying' and by others (e.g., Cross et al., 2009) as 'offline bullying'. Many of these researchers (e.g., Smith et al., 2008) have researched extensively and over a long period of time in the field of bullying.

There will probably never be a perfect definition of bullying that covers every possible set of circumstances and it is unlikely that the differences between definitions can be resolved in any large, international professional group because of the diversity of personal, disciplinary,

cultural and linguistic factors involved (Smith, 2004, 2005). Nevertheless, as Smith (2005) points out, the following criteria are accepted as part of a good working definition by most researchers in the area (Olweus, 1999; Ross, 2002; Smith and Brain, 2000).

- Repeated aggressive actions towards the same specific person or group.
- Distress on the part of the recipient of the aggressive actions.
- An imbalance of power in favour of the person(s) taking the aggressive actions. This means that a fight between equals is not bullying.

The criteria of '*an intention to distress on the part of the person(s) taking the negative/hostile actions'* is also incorporated into many well-established definitions of bullying. In legal terms repetition may in fact *imply* intention (as well as persecution).

Some examples of these more robust definitions of bullying include:

- 'A student is being bullied or victimised when he or she is exposed, repeatedly and over time, to negative actions on the part of one or more students' (Olweus, 1999, p.10).

- 'Bullying is defined … as a repeated, unjustifiable behaviour that may be physical, verbal, and/or psychological. It is intended to cause fear, distress, or harm to another and is conducted by a more powerful individual or group against a less powerful individual who is unable to effectively resist' (Cross, Pintabona, Hall, Hamilton and Erceg, 2004).

- 'Repeated, negative acts committed by one or more children against another' (Limber and Nation, 1998, p.1).

- 'Bullying is when a student (or group) with more power repeatedly and intentionally uses negative words and/or actions against another student that cause distress and create a risk to their wellbeing' (McGrath, 2007).

- 'Aggressive behaviour that is repeated over time, is intentionally harmful and occurs without provocation' (Peterson, 2001, p.2).

- Bullying can be seen as a subtype of aggressive behavior in which a child is exposed repeatedly and over time to negative actions carried out by one or more peers. Bullying is also characterised by an imbalance of power, with a more powerful person or group attacking a powerful one. From this definition it can be derived that bullying is a group phenomenon, taking place in social groups (Sentse, Scholte, Salmivalli and Voeten, 2007).

- Bullying involves a desire to hurt + hurtful action + a power imbalance + (typically) repetition + an unjust use of power + evident enjoyment by the aggressor and a sense of being oppressed on the part of the victim (Rigby, 2008).

Some of the better definitions of cyberbullying that have been adapted from the definitions of general bullying include the following:

- 'An aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself' (Smith et al., 2008, p.376).

- '...a series of incidents by the same harasser (indicating repetition) and either distressing (possibly indicating aggression and imbalance of power) or requiring adult intervention' (Wolak Mitchell and Finkelhor, 2007, p.56).

- Willful and repeated harm inflicted through the medium of electronic text (Hinduja and Patchin, 2006).

- 'An aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself' (Smith et al., 2008, p.376).

- 'Cyberbullying uses information and communication technologies to support deliberate, repeated and hostile behaviour, by an individual or group, which is intended to harm others' (Belsey, n.d).

- 'Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm other' (Belsey, 2008).

- 'Covert psychological bullying conveyed through the electronic mediums... '(Shariff and Gouin, 2005, p.3).

- 'Cyberbullying is bullying which uses e-technology as a means of victimising others. It is the use of an internet service or mobile technologies–such as email, chat room discussion groups, instant messaging, web pages or SMS (text messaging) – with the intention of harming another person'. (South Australian Department of Education and Children's Services, n.d).

Some writers and researchers (Willard, 2007b; Stacey, 2008) have questioned whether the definition of general bullying is too narrow to be used with cyberbullying. One example of this stance is the argument by Willard (2007b) that the approach of adapting the rigorous definition of bullying to cyberbullying may be too narrow, as concepts such as repetition and an imbalance of power do not necessarily capture the nature of many online, socially aggressive activities). Stacey (2008) further argues that not only is *intention* difficult to ascertain in cyberbullying but a single transmission of a humiliating photo or message may bring about responses from others that act like repeated acts of bullying. Others disagree, arguing that a clear concept of repetition is essential to differentiate cyberbullying from a range of other socially aggressive actions. It is arguable, however, that 'repetition' *is* a core component of any type of bullying as it implies persecution. The concept of a 'power imbalance' can be said to be common to both types of bullying, although the nature of the power may be different (Harris, Petrie and Willoughby, 2002; Vandebosch, 2008). Harris, Petrie and Willoughby (2002) argue that sitting behind a computer working the keyboard gives students a sense of power and control that they do not have in a face-to-face situation, especially if they have a higher level of skill than the student they are victimising. In most forms of offline bullying the power imbalance is created by factors such as higher levels of social status and influence, physical strength, age, numbers, a weapon and sometimes verbal superiority. In cyberbullying the power imbalance may still reflect higher social status and numbers of people involved but also includes anonymity and technological skills (Vandebosch and van Cleemput, 2008).

Slonje and Smith (2006) have suggested that some types of more complex online aggression such as posting an offensive image or video clip of someone on a website (or sending it by text message) may only happen on one occasion but may still reflect the essence of repetition (i.e., ongoing persecution) because it involves several intentional steps and (usually) ongoing maintenance (e.g., sending it on to additional people, communicating

the address of the website to others, making further comments about the images on the website etc.). Slonje and Smith (2006) also argue that the essence of repetition is also present if many people (after being told about it) access that specific webpage, it could be argued that this fits the category of repetition. Slonje and Smith (2006) suggest that the more traditional use of 'repetition' as a criterion for bullying may be less reliable for these specific and complex acts of cyberbullying. It is argued in this report that it is the multi-faceted and/or multi-step nature of some complex behaviours that implies persecution rather than the fact that a specific action may result in many people witnessing it because of the potential size of the audience.

A cyberbullying definition per se that is too broad and all encompassing runs the risk of muddying the waters and scaring parents, teachers and the general community into over-reacting to what in some cases is a fairly minor and one-off problem which may just be the online equivalent of a single playground incident (AISV, 2009) or a single act of disrespect or impulse. There is also an associated risk of schools becoming the target of inappropriate legal action if a sloppy definition is used. Most poor definitions make it almost impossible for students, teachers and parents to distinguish genuine cyberbullying from one-off acts of cyber-aggression (referred to as cyber-attacks), mutual conflict (or cyber-fighting) and acts of social non-preference not accompanied by intention to harm. Cyber-attacks are also unacceptable and must still be managed and cyber-fighting must also be discussed and addressed. However cyberbullying often requires a different, more complex relationship-based management approach. As Pepler (2007) notes, 'bullying is a relationship problem that requires relationship solutions' (p.1).

The definitions of cyberbullying that do not include characteristics such as repetition, intention or a specific targeted student (and thereby tend to confuse cyber-attacks and mutual cyber-fighting with cyberbullying) tend to have been developed by writers or researchers with a background in Information and Communications Technology. Some examples are:

- 'Cyber-bullying is the general term describing any communication activity using cyber technology that could be considered harmful to individual or collective well-being' (Bamford, 2004, p.1).

- 'Cyberbullying is being cruel to others by sending or posting harmful material or engaging in other forms of social aggression using the Internet or other digital technologies'' (Willard, n.d.)

- 'Cyberbullying can be defined as the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else' (TeacherNet, n.d.).

- [Cyberbullying is] 'when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person' (National Crime Prevention Council, USA ,n.d.).

How do young people define bullying and cyberbullying?
Vandebosch and van Cleemput (2008) used focus groups to investigate the views of 279 young people (aged 10-18) in 10 schools about what cyberbullying is believed to be. They found that they did not have a clear idea of what cyberbullying is, and tended to equate it with a cyber-attack i.e., a single episode using communication technologies of one kind to be aggressive towards, threaten, insult or humiliate another person.

Monks and Smith (2006) looked at how young people of different ages defined bullying by asking them to decide whether or not cartoons and scenarios depicted bullying or not. They

found that that just over half of the children aged 4-8 years had some understanding of the term 'bullying' but did not include characteristics such as repetition or power imbalance. The other half tended to categorise any acts of aggression and/or fighting as 'bullying'. On the other hand most 14 year olds did understand the concept of bullying, did incorporate criteria such as 'repetition' and 'power imbalance' and could also distinguish between physical and non-physical (i.e., social/relational or verbal) bullying actions.

SIMILARITIES BETWEEN BULLYING AND CYBERBULLYING

The similarities between offline bullying and cyberbullying can be summarised as follows:

- Both offline and cyberbullying are about destructive human relationships, power and social control.
- Many of the same students are victimised both online and offline.
- Most offline bullying actions have a cyberbullying counterpart.
- The motivations for taking part in offline bullying are similar to those for participating in cyberbullying.
- Overall, the level of distress from being bullied offline appears to be similar to the level of distress from being cyberbullied.

Both offline and cyberbullying are about destructive human relationships, power and control.

As Pepler (2007) highlights, bullying is first and foremost about power and those who bully are frequently rewarded for their use of aggression to achieve power. They intentionally create destructive relationships in order to achieve their own ends (Belsey, 2008). In describing adolescence, Pellegrini and Bartini (2000) whilst noting that adolescence can be a brutalising period of development, also highlight that one way in which young adolescents, especially boys, try to achieve peer status is through the selective use of aggression and other antagonistic strategies. Both offline bullying and online bullying offer an opportunity to do this.

Many of the same students are victimised both online and offline.

Research studies conducted so far suggest that students who are bullied offline are also more likely to be targets of cyberbullying (e.g., Cross et al., 2009; Kowalski and Limber, 2007; Raskauskas and Stoltz, 2007; Smith, 2008).

Most offline bullying actions have a cyberbullying counterpart.

Most aggressive actions which, if repeatedly and intentionally directed towards the same person would be considered bullying, have a cyberbullying counterpart, for example:

- Offline sexist, racist and homophobic insults and name-calling usually involves face-to-face-to-face insults or written notes about being a 'fag', a 'wog' or a 'slut'. The same insults can be sent via an MSN or a text message.

- Finding ways to humiliate someone offline may involve a practical joke in which a person's clothes are hidden after a swimming lesson to make someone look stupid. This can also be achieved online by transmitting or uploading a humiliating digital image.

- Damaging social and personal reputations in an offline context may involve everyone getting up and moving away every time a specific student sits nearby. Getting together to repeatedly block someone from a chat room would be the online equivalent.

The motivations for taking part in offline bullying are similar to those for participating in cyberbullying.

Young people decide to cyberbully another person for (mostly) the same reasons as they decide to bully someone offline (Vandebosch and van Cleemput, 2008). These motivations include:

- A desire to enhance their social superiority and impress others with their 'power' by expressing their contempt for the victimised young person's assumed inferiority or weakness. In cyberbullying there may also be a desire to display technological skills and 'power' to others and over others, gain status and 'look good' (Cross et al., 2009; Patchin and Hinduja, 2006).

- Bonding and showing commitment to and acceptance by a friendship group by victimising someone to highlight their lack of acceptance.

- A desire to relieve boredom and have fun together (e.g., Cross et al., 2009; Smith et al., 2008). This can take many forms. In offline bullying someone might arrange to meet a girl/boy by pretending they like them and then not turn up at the arranged place and time. Meanwhile others may have been invited to watch the humiliation of the person who has been set up as they wait. In cyberbullying someone might send a text messages to a girl/boy and pretend to like them and then share their replies with others so they can all 'have a laugh' (although the person who is being humiliated doesn't find it very funny).

Overall, the level of distress from being bullied offline is similar to that from being cyberbullied.

Victimised young people experience the same feelings of powerlessness and humiliation whether they are bullied offline or cyberbullied (Snider and Borel, 2004). There has been speculation that this sense of powerlessness and humiliation may be more extreme in some situations of cyberbullying, especially those that that are complex multi-step campaigns involving the posting or transmission of images. However, Ybarra et al. (2006) note that the impact of cyberbullying relative to offline bullying is still very unclear. A study in the UK (YouGov, 2006) found that 13% of young people who responded to a survey perceived that cyberbullying would be more harmful and distressing than offline bullying and several writers in this area have agreed with this perception (Brown et al., 2006; Campbell, 2005). However, neither Cross et al. (2009) nor Smith et al. (2008) found this to be the case in their studies. In their focus group discussions with students Smith et al. (2008) found that cyberbullying was perceived to be *potentially* more publicly humiliating and harder to escape from and hence it could be *potentially* more distressing than offline bullying, especially if humiliating images were involved. Cross et al. (2009) found that the majority of students in their study perceived that offline bullying would be worse than cyberbullying. Students who have actually been cyberbullied may have different perceptions to the general student population. The possible size of the audience for public humiliation and the difficulty of working out who is doing it might enhance the negative impact of cyberbullying, but the possibility of quickly blocking some forms of electronic bullying (compared to face-to-face harassment) might also lessen the impact in some situations (Smith et al., 2008). Unfortunately suicides and murder are occasionally the end result of distress and humiliation from both types of bullying.

DIFFERENCES BETWEEN BULLYING AND CYBERBULLYING

Although cyberbullying is very similar to offline bullying in many significant ways there are also ways in which cyberbullying appears to be different. In summary these are:

- There may be more disinhibition involved in cyberbullying.

- The potential anonymity of technology may facilitate anti-social behaviour and increase distress.
- It can be harder to escape from cyberbullying.
- Cyberbullying can amplify the impact of being bullied.
- Friends and are less likely to be around to support you when you are being cyberbullied.
- Bystanders may play a lesser role in cyberbullying.
- There is a lack of immediate verbal and non-verbal feedback (and hence lowered empathy) in cyberbullying.
- There may be more opportunity to 'share' cyberbullying.
- Bullying via technology may be perceived by young people as more 'glamorous'.
- It may be easier for young people who have been bullied or cyberbullied to retaliate via the same technology.
- There may be different age trends in cyberbullying.
- Young people who are cyberbullied may be less likely to tell an adult about it.
- Young people may be more likely to cyberbully people they haven't even met and don't know.
- Adults are less aware of cyberbullying as it is nearly always carried out secretly and away from their supervision.
- There appears to be less cyberbullying than offline bullying.
- It is easier to cyberbully teachers than to bully them offline.
- Cyberbullying usually leaves behind more evidence than offline bullying.
- Changing schools may be a less effective approach for students who are cyberbullied.

There may be more disinhibition involved in cyberbullying.
Technology appears to create a type of disinhibition that weakens young people's sense of social accountability and leaves them more vulnerable to peer pressure.

> '… it is becoming clear that aspects of online communication encourage people to act aggressively, prompting them to do things they wouldn't dare to try in real life' (McKenna, 2007, p.60).

In a study conducted by Pew, Internet and American Life Project (Lenhart, Maddden and Hitlin, 2005), more than one-third of the adolescents who reported using instant messaging admitted to saying things they would not normally say in face-to-face conversations. Some of the disinhibition may derive from the assumption of technological anonymity (as discussed in the next point) that may contribute to a reduced sense of social accountability (Herring, 2001; Vandebosch et al., 2008). Lee (2008) cites the high levels of looting and rape that occurred during the 1965 New York blackout, when people were more able to conceal their identity, as a similar example.

The potential anonymity of technology may facilitate anti-social behaviour and increase distress.
Ybarra and Mitchell (2004) point out that one significant difference between cyberbullying and offline bullying is the ability for those engaged in cyberbullying to withhold their identity in cyberspace. This provides a 'unique method of asserting dominance online that conventional bullying disallows' (p.1313). The potential to withhold one's own identity (e.g., by setting your phone to 'number withheld', having several email address, assuming several alternate identities or using someone else's identity) can create opportunities for young people to communicate in abusive ways online and when using a mobile phone that they might not normally choose to use in face-to-face encounters (Berson and Berson, 2005; McKenna and Bargh, 2000; Patchin and Hinjua, 2006; Willard, 2003). This may also make them more susceptible to anti-social peer pressures.

There are many ways in which someone can (seemingly) remain anonymous when cyberbullying another person. It is relatively easy for someone with a reasonable level of

27

technological skills to impersonate another, use an avatar or create a false identity or a pseudonym to operate behind. Belsey (2008) claims that those who cyberbully anonymously are more cowardly. Being anonymous protects, to some extent, the person(s) involved in the cyberbullying as they assume they will not have to take the consequences of their actions (Brown et al., 2006; Ybarra and Mitchell, 2004a). This may be especially true if students undertake cyberbullying when they are not on school grounds and outside school hours. However changes to legislation and the rights and responsibilities of schools are now challenging this assumption.

If the person who is being victimised does not know who their tormentors are they may find it more difficult to respond to what is happening to them in a constructive way and may forced to limit or temporarily stop their use of the internet or mobile phone. This may make a young person's life very miserable, socially isolate them even further and lead to feelings of powerlessness. On the other hand, knowing who it is enables some perspective and allows them to more clearly consider their response strategy (Vandebosch and van Cleemput, 2008). The students in the focus groups conducted in the study by Smith et al. (2008) reported that anonymous cyberbullying could make some students more frightened. Cross et al. (2009) also reported that, although the majority of students in their study perceived that offline bullying involving name-calling was worse than cyberbullying, the *aspect* of cyberbullying that concerned them the most was not knowing who was doing the cyberbullying (56%) followed by the public humiliation (26%). If the content of anonymous communications is also threatening, the degree of fear may be even higher (Campbell, 2005). Not knowing who is tormenting and humiliating you can also lead to social insecurity. Is it a friend doing this, an enemy, the person who sits next to you in class, or most of your year level? A young person's trust in others can quickly be undermined and he/she may doubt their ability to identify their real friends. Kowalski and Limber (2007) reported that nearly half of the students they interviewed who had been cyberbullied did not know who had done it to them.

To some extent this kind of anonymity is really 'pseudoanonymity' (Berson and Berson, 2005) as digital footprints always remain as clues to identity. However they may be difficult to retrieve in many cases (Willard, 2004) and schools may perceive that the outcome may not justify the effort. However, Vandebosch and van Cleemput (2008) found that some students in their study reported that those who had been cyberbullying anonymously sometimes 'outed' themselves (perhaps for the satisfaction and sense of power obtained by letting peers know what they had been able to do) and in other cases those who had been present when cyberbullying occurred anonymously (or who knew about it in other ways) revealed to teachers or parents who was behind it.

It can be harder to escape from cyberbullying.
Cyberbullying can be relentless in that it can happen not only at school but also at home and out of school hours. Opportunities for cyberbullying are not limited by time or place and most cyberbullying does appear to occur outside school (e.g., Smith et al., 2008). For students who are cyberbullied there is no safety, refuge or respite at home and this is part of the pain that accompanies it (Cross et al., 2009).

Cyberbullying can amplify the impact of being bullied.
Cyberbullying can be enacted speedily (and sometimes instantaneously) and attract a very large audience. It can reach many people both in the short term and over an extended period of time. Those who choose to cyberbully are not constrained by the need to be in the same place at the same time as the person they victimise. The cruelty can be inflicted from anywhere he/she has the technology and at any time (Bauman, 2007). The nasty and humiliating products of some types of cyberbullying (e.g., text and images) can be sent on

to others, downloaded, cut and pasted and kept by many people to look at and talk about over and over again. The recipient unfortunately can also revisit the products and re-live the experience many times resulting in a more prolonged sense of victimisation which may lead to depression (Brown, Jackson and Cassidy, 2006). For some victimised students there may never be any certainty that humiliating text or images aren't still circulating somewhere in cyberspace and may be re-broadcast at a later time. Campbell (2005) argues that, in comparison, offline bullying, although distressing at the time it occurs, often fades and words and taunts become vague and less painful. This is an area yet to be clarified.

Your friends and are less likely to be around to support you when you are being cyberbullied.

Since cyberbullying can be done anywhere and anytime there is a lower likelihood that a young person's friends will be with them when they are being cyberbullied so there is less opportunity for friends to provide immediate support and help to moderate the impulse towards retaliation which can escalate the cyberbullying.

Bystanders may play a lesser role in cyberbullying.

The actions and words of bystanders (i.e., those who witness what occurs or are aware of what is occurring) can have a significant effect in minimising and terminating offline bullying behaviours. However 'bystanders' probably have less impact in cyberbullying as it is more likely to occur whilst the perpetrator is alone or in the presence of their friends rather than in the presence of a wide range of peers, some of whom may not be in their friendship group. In cyberbullying bystanders can readily become 'accessories' and become involved, for example, by passing on or showing to others nasty text or images designed to humiliate, or by taking part in online polls or discussion groups. They may not immediately recognise that they are participating in cyberbullying (TeacherNet, n.d.).

There is a lack of immediate verbal and non-verbal feedback (and hence lowered empathy) in cyberbullying.

Another significant difference between offline bullying and cyberbullying is the lack of immediate verbal and non-verbal feedback from the victimised person when they are cyberbullied. Without this feedback empathy for the recipient is lowered and it is easier to do it again (Belsey, 2005; Brown et al., 2006; Kowalski, Limber and Agatson, 2008; Smith et al., 2008; Willard, 2004, 2006). McKenna (2007) notes that seeing the pain and distress of the person towards whom you are directing cruel behaviour can act as an inhibitor to some degree but that lack of face-to-face contact may tempt those who start to cyberbully to move to even higher levels of cruelty as they are more able to distance themselves from their victim as though what they are doing isn't 'real'.

There may be more opportunity to 'share' cyberbullying.

A young person who cyberbullies can more readily share what they have done with their peers than they can when they have bullied in more traditional ways (Smith et al., 2008). For example they may get some peer reinforcement through sharing pictures, text messages, emails and video clips, thus amusing others in their social group and thereby starting to construct the wider audience often involved in cyberbullying (Smith et al., 2008).

Bullying via technology may be perceived by young people as more 'glamorous'.

Cyberbullying may seem more glamorous to young people for several reasons. As noted earlier young people may over-value any actions undertaken using technology as many of them perceive that they have skills that are better than those of many of the adults around them (Bauman, 2007). Contemporary social norms may foster online misbehaviour because it is an aspect of the social world of young people, especially those who still have limited freedom to socialise.

It may be easier for young people who have been bullied or cyberbullied to retaliate via technology.
Students who have been on the receiving end of offline bullying at school as well as those who have been cyberbullied may find it easier to retaliate against their persecutors online than in person. Retaliation via electronic means may be less physically dangerous than face-to-face retaliation (Smith et al., 2008). Although they may be less articulate than their tormentors, they may have the same familiarity with technology and equal or superior technological skills. They may feel entitled to respond in kind if they have been cyberbullied. The cycle may then escalate and lead to more serious situations. Ybarra and Mitchell (2004b) believe that the disinhibition process that enables students to cyberbully also enables some victimised young people to retaliate online for the cruelty to which they have been subjected.

There may be different age trends in cyberbullying.
It has been suggested that cyberbullying may produce different age trends from those identified in offline bullying as technological access, familiarity, confidence and skill increases with age. Studies by Cross et al. (2009), Smith et al. (2008) and Ybarra and Mitchell (2004b) have found that students are more likely to become involved with 'one off' as well as repeated internet aggression as they got older, with a possible peak occurring between 13-15+ years (Smith et al., 2008).

Young people who are cyberbullied may be less likely to tell an adult about it.
Although students who are bullied offline can also be reluctant to tell an adult what is happening to them students who are cyberbullied appear to be (possibly) even more reluctant to tell an adult about what is happening (Cross et al., 2009; Li, 2007; Smith et al., 2008). Belsey (2008) believes that many may fear that, in response, adults will over-react and remove their private access to communication technologies. Being denied this access would mean potential social exclusion through being unable to communicate and socialise with peers. Cross et al. (2009) have also identified that students' reluctance to tell an adult about being cyberbullied may reflect their concerns about adults' heavy-handedness, inaction or the potential retaliation that may occur.

Young people may be more likely to cyberbully people they haven't met and don't know.
In their study of young people between 10 and 18 years of age, Vandebosch and van Cleemput (2008) discovered that cyberbullying was sometimes directed towards other young people who were total strangers. For example some of the people in their focus groups spoke of taking on another identity to intentionally and regularly mislead other young people who they met in chat rooms or of sending a number of insulting or threatening messages to the email address of someone they had never met. Sometimes the selection of unknown targets was made randomly but in other cases the selection was more strategic and based on the perceived 'weaknesses' of the online strangers. For example they might be selected because they were younger or inexperienced girls. Subjecting strangers to cruelty for the fun of it can also occur using offline bullying tactics but it is probably less likely as an unknown 'target' could prove to be dangerous in person.

Adults are less aware of cyberbullying than they are of offline bullying as it is nearly always carried out secretly and away from their supervision.
Teachers and parents have always had difficulty in identifying when any type of bullying occurs because it tends to be carried out when and where adults are unlikely to witness it or become aware of it. This is even more true of cyberbullying.

There is less cyberbullying than offline bullying.
In their respective studies with young people both Cross et al. (2009) and Smith et al. (2008) found that cyberbullying happens less often than offline bullying.

Cyberbullying usually leaves behind more evidence than offline bullying.
Cyberbullying can be 'proven' more readily than offline bullying because 'products' can usually be provided and digital footprints can be tracked and identified. The recipients can print and keep vicious emails that have been sent to them. They can use 'screen capture' to take a photograph of the screen when printing isn't an option. They can download digital images that have been posted to humiliate them.

It is easier to cyberbully teachers than to bully them offline.
Offline bullying, usually in the form of practical jokes or spreading rumours, can be directed towards teachers but cyberbullying is easier to do. As discussed earlier in this review (under '*Legal Issues*') there have been several documented cases in the UK of students posting offensive images and abusive and false information about teachers online (Frean, 2007).

Changing schools may be a less effective strategy for students who are cyberbullied.
Changing schools can be an effective strategy for escaping from bullying for some young people. However this is less likely to be effective in situations of cyberbullying as their persecutors will (mostly) still be able to cause them harm in the wider cyberworld.

THE PREVALENCE OF CYBERBULLYING
To date only a small amount of research has been carried out to investigate the prevalence of cyberbullying and the factors associated with it. Much of the research that has been conducted contains serious limitations including a lack of conceptual clarity (Vandebosch and van Cleemput, 2008). There are several reasons for this.

- *C*yberbullying is a relatively new phenomenon and the survey questions used in studies are very inconsistent. There are no existing measures of cyberbullying that have undergone rigorous psychometric study (Diamanduros et al., 2008, p.697).

- *C*yberbullying has been defined in several different ways (as described earlier in this review) and the way in which it is defined has implications for how it is measured. Many studies use very poor surveys which have one or more of the following limitations:

    - They do not provide the respondents with a clear definition of what cyberbullying is to guide them in their responses.
    - They ask simple questions such as, "*Have you <u>ever</u> been cyberbullied*?" as though a one-off cyber-attack is also an example of cyberbullying.
    - Similarly, they provide response options such as "*I have been cyberbullied once.*", thereby implying that you can have a single incident of cyberbullying.
    - One question often asked is "*Have you seen or heard about someone being cyberbullied?*". Many students who respond in the affirmative may be answering with the same person/example in mind, hence inflating the percentages.

- In some research studies respondents *are* provided with a very sound definition to start with, but are then asked survey or interview questions such as those above which don't reflect the definition given.

- Some research studies appear to *combine* bullying and cyberbullying as a focus for their study and ask, "*How often have you been bullied?*" as well as, "*How often have you been cyberbullied?*" The confusing assumption here seems to be that the cyberbullying might only happen once, but it must be part of an overall bullying pattern being directed towards an individual so it can be measured in this way.

Different assumptions about what cyberbullying actually is have also led to different kinds of research methodology (Vandebosch and van Cleemput, 2008) and, inevitably, to inconsistent research results, especially in regards to the prevalence of cyberbullying (Vandebosch and van Cleemput, 2008). Several studies have attempted to study cyberbullying via online surveys or school-based surveys in which young people are asked about their experiences (as someone who bullies, someone who is bullied or as a bystander). A typical question might be "*How often have you been bullied by mobile phone?"* In other studies the term 'bullying' isn't introduced as a concept but cyberbullying is *assumed* from the respondents' reported (and often only one-off) negative experiences (or a single experience) with a range of activities using communications technology tools which are *assumed* by the researcher to represent cyberbullying (e.g., being insulted by a classmate, perhaps only once, via text message or instant messaging).

As a result of these differences and limitations we have data that suggests that somewhere between 4% and 42% of all young people are cyberbullied (Beran and Li, 2005; Cross et al., 2009; Hinduja and Patchin, 2008; i-Safe National Assessment Center, 2006; Lenhart, Maddden and Hitlin, 2005, 2007; Smith et al., 2008) The lack of consistent data from robust studies is clearly problematic and unhelpful. The results from three studies are reported here.

Smith, Mahdavi, Carvalho, Fisher, Russell, and Tippett (2008)
This robust study involved two surveys with UK students aged 11–16 years and quantitative data was supplemented with focus group discussions with students. Results included:

- Students reported lower levels of being cyberbullied (5-10%) than of being bullied offline.
- More cyberbullying occurred outside school hours and off the school site than during school hours and onsite.
- The most frequently used technological bullying tools were phone calls, text messages and instant messaging.
- Most cyberbullying was carried out by one student or a few students usually from the same year group. It was usually relatively short-lived i.e. it lasted for about a week (but sometimes much longer).
- In 80% of cases of cyberbulling the identity of those taking part in the victimisation (usually between 1-3 students) is known.
- 48% of students who had been cyberbullied did not tell anyone.

Microsoft Australia (2008)
Galaxy Research (2008) conducted research into cyberbullying on behalf of Microsoft Australia with 300 young people aged 10-17 years. However no details appear to have been published as to how their surveys were carried out, what questions were asked and whether a definition of cyberbullying was provided. They found that:

- One quarter of the young people in the study reported that they had been cyberbullied.
- 31% of the young people who were aged between 4-17 years reported being cyberbullied compared to 21% of those aged 10-13 years.
- Two thirds of the children who said they had been cyberbullied said that they had told their parents while those who did not do so cited their fear of having their internet use reduced or blocked as the reason.
- More than 57% of parents and 59% of children said that they had heard of incidents of cyberbullying among people they know.

Cross et al. (2009)
In their extensive Australia-wide survey of young people in years 4 through to Year 8, the researchers found that between 7% and 10% of students were cyberbullied each term, mainly via nasty text and instant messaging. The use of social networking sites to cyberbully increased with age. Secondary students were more likely to be cyberbullied than primary students. Students who reported being cyberbullied were:

- 13 times more likely to be bullied offline as well and 4 times more likely to cyberbully others;
- twice as likely to have their own mobile phone;
- nearly twice as likely to have wireless internet at home and to report poor academic results;
- more likely to report feeling lonely at school and less connected to school; and
- more likely to perceive their school as taking less action to stop bullying.

On the other hand students who reported that they cyberbullied others were:

- 18 times more likely to bully others offline as well;
- 4 times more likely to be cyberbullied themselves; and
- nearly 3 times more likely to have their own mobile phone.

YOUNG PEOPLE AND SEXUAL PREDATION
In summary
The potential danger to young people from online sexual predators is real and serious but the situation is more complex and less frightening than originally thought. Sexual predation of very young children by paedophiles (i.e., those who are sexually attracted to children under 12 years of age) appears to be relatively rare. Internet predators are either the same age as their targets or approximately 5- 10 years older. They tend to target young adolescents and usually use e seduction and romance rather than deception and coercion. Young people may be more responsible and self-protective in the way they use technology than previous studies have suggested and hence less likely to be targeted by internet predators.

There appears to have been an exaggeration of (and hence an overreaction to) the dangers of new technology, especially those related to 'internet stranger danger' i.e., internet sexual predators (ISTTF, 2008). This conclusion is based on the outcomes from three American studies conducted by the *Crimes against Children Research Center* at the University of New Hampshire in Durham (Wolak, Finkelhor, Mitchell, and Ybarra, 2008). Two of these studies involved contacting 3,000 young internet users (10-17 years old) firstly in 2000 and then again in 2005. Another study involved 612 interviews with investigators from a nationally representative sample of agencies in the USA that deal with the internet. This conclusion has also been endorsed in the final report (released on January 31st, 2009) of the ISSTF (2008) entitled '*Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States.* The ISTTF was a multi-state working group which consisted of attorneys general from many different states in the USA plus internet companies such as MySpace, Facebook, Yahoo!,Google and AOL.

Some of the more specific details of the conclusions from both the ISSTF report (2008) and the studies conducted by Wolak et al. (2008) include:

- Internet-related sex crimes are a very small proportion of sex crimes committed against young people. Sexual assaults against young people in the USA aged 13-18 actually decreased 52% from 1993 to 2005 according to official data.

- Internet predators are rarely paedophiles i.e., people who are sexually attracted to children below the age of 12 years. Internet predators tend to target young girls aged 13-17 years old or young boys of the same age who are uncertain about their sexual orientation. Young people of this age have more access to computers, more privacy and more interest in sex and romance. The offenders use internet a range of online communications such as instant messages, email, and chat rooms to meet and develop intimate relationships with their targets. However in most cases, the young people who are targeted are aware they are conversing online with adults.

- Young people who respond to their overtures are more likely to have a pattern of risk-taking both off- line and online or a history of being abused as children.

- The main crime that follows from internet predation is that of non-forcible statutory rape, i.e., having sexual contact with a minor who is deemed by law to be too young to consent. This is a serious concern.

- Internet predators rarely trick or abduct their targets and although some pretend online to be the same age as their target they are often recognised as being older.

- Some of the targeted young people who respond to these sexual solicitations agree to in-person meetings but most appear to do so expecting to engage in some kind of sexual activity.

Many teenagers frequently interact safely online with people they don't know as part of the development of their identity. They clearly need to be made aware that it is risky to provide names, phone numbers and pictures to strangers and to talk online with them about sex. However, a study by Hinduja and Patchin (2008) analysed a publicly viewable sample of 1475 online user profiles of young people in MySpace and found that only 8.8% revealed their full name, 57% included a picture, 27.8% listed their school and only 0.3% provided their phone number. Their conclusion was that the vast majority of the young people seemed to be behaving in a responsible way when using a social networking website.

DOES INTERNET ADDICTION EXIST?
In summary
Young (1998) originally proposed the term 'Internet Addiction Disorder' and developed the *Diagnostic Questionnaire for Internet Addiction (*YDQ) which she adapted from the criteria outlined in the DSM IV (1994) for 'pathological gambling', which is cited in the DSM IV-TR (2000) as an example of an Impulse Control Disorder. However, although there is a small number of writers and researchers (especially in China, Taiwan and Korea) who claim that this is an identifiable behavioural syndrome, there is no sound research evidence nor convincing theoretical support for such a syndrome at this time. It has been suggested that 'internet addiction' is a term that has been promoted and sensationalised by the media but as yet has little clinical validity

There is no official psychological or psychiatric diagnostic syndrome called 'Internet Addiction Disorder'. The most recent edition of the *Diagnostic and Statistical Manual of Mental Disorders*, DSM-IV-TR (2000), does not include such a diagnostic category. The DSM IV is published by the American Psychiatric Association (APA) and provides diagnostic criteria for mental disorders/syndromes. It is used extensively around the world as the diagnostic 'bible' by clinicians, researchers, agencies that regulate psychiatric drugs, legal systems and health insurance companies. The research and theory for all of both proposed and established disorders are continually monitored by the APA and each new version contains some deletions, revisions and additional disorders. The next version (DSM-V) is due for release in

34

2012. 'Internet Addiction Disorder' could only be accepted as a disorder if research was able to demonstrate that such a syndrome can be reliably measured and established as significantly different from existing disorders, and that the diagnosis has external validity in that it reliably correlates with treatment outcomes, case histories and prognosis.

The following are some of the difficulties with the concept of 'Internet Addiction Disorder':

- Sound published studies on internet addiction are scarce. Most have been conducted by Chinese and Korean researchers, perhaps reflecting the publicised concerns in those countries about what has been described as excessive use of the internet (mainly for online gaming purposes) in the millions of very large internet cafes that have been established. For example in August 2005, the BBC reported the death of a young Korean man who had continuously played online games in an internet café for 50 hours, neglecting to eat, drink and sleep. Most studies are based only on surveys, using self-selecting samples but no control groups. Some of the other published papers on internet addiction are theoretical papers that speculate on the philosophical aspects of internet addiction but provide no data (De Angelis, 2000).

- There certainly have been speculations that some of the unique aspects of the internet may lure people into difficulties they might otherwise avoid such as online gambling, accessing of pornographic sites and the development of inappropriate sexual relationships ('cyber-affairs'), online auctions and online shopping. However it isn't enough to simply describe an activity that people can spend too much time on, or engage in to excess on occasions as an 'addiction'.

- Different researchers in each country have developed their own scales and there are at least five different scales available.

- There is no research evidence that a passion for the internet is long-lasting, nor that excessive internet usage isn't simply a reflection of a problem such as social phobia or loneliness.

- Many of the strongest proponents for establishing that the category of internet addiction *does* exist separate from other disorders have some commercial interest in doing so. For example Kimberley Young (1998), who first proposed the disorder and developed the first questionnaire, runs a private centre to treat excessive internet usage and train others to do so (http://www.netaddiction.com). Dr Jerald Block, an American psychiatrist who is one of the strongest advocates for the inclusion of Internet Addiction Disorder in the next version of the DSM also disclaims that he "…owns a patent on technology that can be used to restrict computer access" (Block, 2008). Greenfield (1999) surveyed 18,000 internet users who logged onto the ABC News Web site and found that 5.7% of the self-selected respondents met the supposed criteria for compulsive internet use but he has, for some time, also had a private centre which provides treatment and training (www.virtual-addiction.com).

- Several Chinese, Taiwanese and Korean researchers who have surveyed young people (mostly aged 12-18) using one of the many questionnaires that purport to measure internet addiction have found some interesting co-occurring behaviour patterns. Their results suggest that those young people whose scores on these various tests suggest they are 'addicted' to the internet have a range of other symptoms as well. In particular a pattern emerges in which those with supposed internet addiction also have scores on other measures which suggest they also have symptoms of ADHD, show high levels of impulsiveness, social phobia, hostility, depression, hyperactivity and emotional problems, and lack pro-social behaviour (e.g., Cao et al., 2007; Yen et al., 2007; Yoo et al., 2004). Yen et al. (2007) conclude

that many of these characteristics (e.g., depression) are the *result* of internet addiction. Yoo et al. (2004) have suggested that some of these characteristics may be *risk factors* for internet addiction while Cao et al. (2007) argue that such characteristics may indicate the presence of psychiatric disorders which are *co-morbid with internet addiction* (i.e., they occur simultaneously but are not necessarily related to each other). However it makes more sense to assume that excessive internet usage may be a *symptom* of disorders which are already included in the DSM IV –TR such as ADHD, Social Phobia or Depression.

It is also possible that at a later point 'excessive internet usage' may be given as an additional example of an Impulse Control Disorder. This disorder already exists in the DSM IV-TR and currently includes examples such as: compulsive gambling, pyromania, trichotillomania (hair pulling), gambling, kleptomania & intermittent explosive disorder (in which the person has outbursts of uncontrollable rage). Impulse control disorders sometimes have characteristics that are also common in other disorders and often occur in conjunction with other conditions, such as ADHD or conduct disorder (Sisk, 2006).

References

ACMA (Australian Communications and Media Authority), December, 2007, *Media and Communications in Australian Families 2007*: Report of the Media and Society Research Project.

Adams, S., 2007, 'Cyber-bullying: An emerging form of student aggression for the 'always-on' generation', *The Australian Educational Leader,* vol. 29, no. 2, pp. 16-19, 41-42.

AISV (Association of Independent Schools in Victoria), 2009, 'The AISV CyberCulture Survey 2008: Preliminary survey results*', AISV Research Brief,* 3, 1, 1-4 February

DSM IV (Diagnostic and Statistical Manual of Mental Disorders-4th Edition), 1994, APA (American Psychiatric Association).

DSM IV-TR (Diagnostic and Statistical Manual of Mental Disorders-Text Revision), 2000, APA (American Psychiatric Association).

Bamford, A., 2004, '*Cyber-Bullying'*, Paper presented at the AHISA Pastoral Care National Conference. Melbourne 2004. Retrieved January 18th, 2009 from: http://www.coc.edu.au/site/_documents/ahisaconference-bamfordcyberbullying.pdf

Baruch, Y., 2005, 'Bullying on the Net: adverse behavior on e-mail and its impact', *Information and Management,* 42:361–71.

Bauman, S., 2007, '*Cyberbullying: a Virtual Menace',* Paper presented at the National Coalition Against Bullying National Conference, November 2 – 4, 2007, Melbourne, Australia. Retrieved January 16th, 2009 from: http://www.ncab.org.au/pdfs/NCAB%20papers/Workshops/Bauman,%20Dr%20Sheri%20-%20Cyber%20Bullying%20The%20Virtual%20Menance.pdf

Beebe, T.J., Asche, S.E., Harrison, P.A. and Quinlan, K.B., 2004, 'Heightened vulnerability and increased risk-taking among adolescent chat room users: Results from a statewide school survey', *Journal of Adolescent Health, 35,*116-123.

Belsey,B., *Always On, Always Aware.* Retrieved March 26th, 2009 from:www.cyberbullying.org

Belsey, B., 2008, 'Cyberbullying: An Emerging Threat to the "always on" Generation', *Canadian Teacher Magazine*, 18-20.

Beran, T. and Li, Q., 2005, 'Cyber-harassment: a new method for an old behavior', *Journal of Educational Computing Research,* 32(3), 265–277.

Berson, I., 2003, 'Grooming cybervictims: The psychosocial effects of online exploitation for youth', *Journal of School Violence,* 2(1), 5-18

Berson, I. and Berson, M., 2005, 'Challenging Online Behaviors of Youth', *Social Science Computer Review,* 23(1), 29-38.

Best, D., 2007, 'Court Takes Tough Stance on Bullying – Cox v State of New South Wales' [2007] NSWSC 471. *Carter Newell Lawyers: Insurance*. Retrieved March 3rd, 2009 from: www.carternewell.com/media/6764/ins2%200507.pdf -

Block, J., 2008, Editorial: 'Issues for DSM-IV: Internet Addiction', *American Journal of Psychiatry*, 165: 306-307

Brown, K., Jackson, M. and Cassidy, W., 2006, 'Cyber-bullying: Developing policy to direct responses that are equitable and effective in addressing this special form of bullying', *Canadian Journal of Educational Administration and Policy,* 57, Retrieved February 6th, 2009 from: http://www.umanitoba.ca/publications/cjeap/articles/brown_jackson_cassidy.html

Campbell, M.A., 2005, 'Cyber-bullying: An old problem in a new guise?', *Australian Journal of Guidance and Counseling, 15,* 68-76.

Cao, F. and Su, L., 2007, 'Internet addiction among Chinese adolescents: prevalence and psychological features', *Child: Care, Health and Development,* Volume 33, Number 3, May 2007 , pp. 275-281(7)

Childwise, 2009, '*The 2008/2009 Monitor Report',* Retrieved May 1st, 2009 http://www.childwise.co.uk/childwise-published-research-detail.asp?PUBLISH=4'

Cross, D., Pintabona, Y., Hall, M., Hamilton, G. and Erceg, E., 2004, 'Validated guidelines for school-based bullying prevention and management', *International Journal of Mental Health Promotion, 6*(3), 34-42.

Cross, D., Shaw, T., Hearn, L., Epstein, M., Monks, H., Lester, L. and Thomas, L., 2009, '*Australian Covert Bullying Prevalence Study (ACBPS)',* Child Health Promotion Research Centre, Edith Cowan University, Perth. Retrieved June 4th, 2009 from: http://www.deewr.gov.au/Schooling/NationalSafeSchools/Pages/research.aspx

DeAngelis, T., 2000, 'Is Internet Addiction Real?', *Monitor on Psychology,* Volume 31, No. 4, April 2000

Department of Education and Children's Services, South Australia (DECS), n.d., Retrieved March 26th, 2009 from: http://www.decs.sa.gov.au/docs/documents/1/CyberBullyingECrimeProtec.pdf.

Diamanduros, T., Downs, E. and Jenkins, S. J., 2008, 'The role of school psychologists in the assessment, prevention, and intervention of cyberbullying', *Psychology in the Schools*, 45, 693-704

Ford, D., 2007, '*Cyber bullying',* Emil Ford & Co - Lawyers, Sydney. Retrieved April 3rd, 2009 from: http://www.emilford.com.au/web/documents/Cyber-Bullying.pdf

Frean, A., 2007, 'Teachers to sue over online humiliation at hands of pupils', *The Times,* April 4. Retrieved April 14th, 2009 from: http://www.timesonline.co.uk/tol/life_and_style/education/article1610447.ece

Galaxy Research (For Microsoft Australia), 2008, 'Coping with cyberbullying difficult for four out of five parents', *Australian Information Technology, August, 2008.* Retrieved March 26th, 2009 from: http://download.microsoft.com/documents/australia/publicaffairs/August2008.pdf

Greenfield, D.N., 1999, 'Psychological characteristics of compulsive Internet use: a preliminary analysis', *Cyber Psychology and behavior,* 2, 5, 403-412.

Grinter, R. E. and Palen, L., 2002, '*Instant Messaging In Teen Life',* Paper presented at the

Computer Supported Cooperative Work conference, November 16-20, 2002, New Orleans, LA.

Gross, E., Juvonen, J. and Gable, S., 2002, 'Internet Use and Well-Being in Adolescence', *Journal of Social Issues,* 58(1), 75-90.

Hale, E., 2009, 'Gen Y having sex earlier but babies later', *Sunday Herald Sun,* February 15, 2009. Retrieved March 26th, 2009 from: www.news.com.au/heraldsun/story/0,21985,25054197-661,00.html

Harmon, A., 2004. 'Internet gives teenage bullies weapons to wound from afar', *The New York Times (August 26th, 2004)*. Retrieved March 26th, 2009 from: http://www.nytimes.com/2004/08/26/us/internet-gives-teenage-bullies-weapons-to-wound-from-afar.html

Harris, S., Petrie, G. and Willoughby, W., 2002, 'Bullying among 9th graders: An exploratory study', *NASSP Bulletin,* 86(630), 3-14.

Herring, S., 2001. 'Gender and power in online communication', Center for Social Informatics Working Papers. Retrieved March 30th, 2009 from: http://rkcsi.indiana.edu/archive/CSI/WP/WP01-05B.html

Herring, S.C., Scheidt, L.A., Bonus, S., and Wright, E., 2004, '*Bridging the gap: A genre analysis of weblogs',* Paper presented at the Proceedings of the 37th Hawaii international conference on system sciences (HICSS-37), Los Alamitos, CA. Retrieved March 30th, 2009 from: http://www.blogninja.com/DDGDD04.doc.

Hinduja, S. and Patchin, J., 2009, '*Cyberbullying: Legal and policy issues'*, Retrieved March 28th, 2009 from: http://www.cyberbullying.us/cyberbullying_legal_issues.pdf

Hinduja, S. and Patchin, J., 2008, 'Cyberbullying: An exploratory analysis of factors related to offending and victimization', *Deviant Behavior,* 29(2),1-29

Huffaker, D.A. and Calvert, S.L., 2005, 'Gender, identity, and language use in teenage blogs', *Journal of Computer-Mediated Communication, 10*(2), article 1. Retrieved January 30th, 2009 from: http://jcmc.indiana.edu/vol10/issue2/huffaker.html

i-Safe National Assessment Center (2006). '*At risk online: National assessment of youth on the internet and the effectiveness of i-safe internet safety education'*, Retrieved February 9th, 2009 from: http://www.i-safe.org/imgs/pdf/outreach_press/2006_National_Assessments.pdf

Ipsos Reid, February 27th, 2008, '*Inter@ctive Teens: The Impact of the Internet on Canada's Next Generation',* Retrieved January 28th, 2009 from: http://www.ipsos-na.com/news/pressrelease.cfm?id=3829

Ipsos Reid and Microsoft, 2006, '*Untangling The Web: The Facts About Kids And The Internet.'* Retrieved March 18th, 2009 from: http://www.marketwire.com/mw/rel_ca_print.jsp?id=577169

ISTTF, 2008, '*Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States',* The Berkman Center for Internet and

Society, Harvard University. Retrieved April 11th 2009, from:
http://cyber.law.harvard.edu/research/isttf

Kim, J-W., 2005, '*Another big 'Big Brother' in Korean cyberspace: the internet real-name system'*, Association for Progressive Communications, Internet and ICTs for Social Justice and Sustainable Development. Retrieved March 11th, 2009 from:
http://www.apc.org/en/news/strategic/world/another-big-big-brother-korean-cyberspace-internet

Kowalski, R.M. and Limber, S., 2007, 'Electronic Bullying Among Middle School Students', *Journal of Adolescent Health*, 41,22–30

Kowalski, R. M., Limber, S. P., and Agatston, P. W., 2008. '*Cyber bullying: Bullying in the digital age.'* Blackwell Publishing

Lenhart, A., Madden, M., and Hitlin, P., 2005*,* 'Teens and technology: Youth are leading the transition to a fully wired and mobile nation', Washington, DC: *Pew Internet and American Life.* Retrieved March 5th, 2009 from:
http://www.pewinternet.org/Reports/2005/Teens-and-Technology.aspx

Lenhart, A., Madden, M., and Hitlin, P., 2007, 'A Timeline of Teens and Technology', Washington, DC: *Pew Internet and American Life*. Retrieved April 3rd from:
http://www.pewinternet.org/Presentations/2007/A-Timeline-of-Teens-and-Technology.aspx

Li, Q., 2007, 'New bottle but old wine: A research on cyberbullying in schools', *Computers and Human Behavior,* 23(4), 1777-1791

Limber, S. and Nation, 1998, 'Bullying among children and youth', *Juvenile Justice Bulletin.* Retrieved February 11th, 2009, from:
http://www.ojjdp.ncjrs.org/jjbulletin/9804/bullying2.html

McKenna, P., 2007, 'The rise of cyberbullying', *New Scientist,* 7/19/2007, Vol. 195, Issue 2613, 26-27. Retrieved February 11th, 2009 from:
http://www.newscientist.com/article/mg19526136.300-the-rise-of-cyberbullying.html?full=true

McKenna, K.Y.A., and Bargh, J.A., 2000, 'Plan 9 from Cyberspace: The implications of the Internet for personality and social psychology', *Personality and Social Psychology Review,* v4. 57-75.

McCrindle, Mark, n.d., '*Understanding Generation Y'*, The Australian Leadership Foundation. Retrieved April 13th, 2009 from:
http://www.mccrindle.com.au/wp_pdf/BridgingTheGap.pdf

McGrath, H., 2007, '*Making Australian Schools Safer: Summary Report of the National Safe Schools Framework Best Practices Grants Programme*'. Retrieved February 8th, 2009 from: www.dest.gov.au/sectors/school_education/publications_resources/.../National_Safe_Schools_Framework_Best_Practice.htm

Microsoft and Ipsos Reid, 2007, '*Children Misunderstand Public Nature of The Internet, Survey Finds' (*January 24th, 2007). Retrieved February 3rd, 2009 from:
http://www.microsoft.com/canada/media/releases/2007_01_24.mspx

Monks, C.P. and Smith, P., 2006 'Definitions of bullying: Age differences in understanding of

the term and the role of experience', *British Journal of Developmental Psychology* 24, 801–821

National Crime Prevention Council, n.d, '*Cyberbullying',* Retrieved February 11th 2009, from: http://www.ncpc.org/cyberbullying

NetAlert, n.d. '*Protecting Australian Families Online',* Retrieved February 11th 2009, from: www.netalert.gov.au,

NetSafeKids, n.d. '*Protecting Children From Pornography and Sexual Predators on the Internet*', Retrieved January 29th from: http://www.nap.edu/netsafekids/

NetSafe, NZ, n.d. 'School Cybersafety Policy Template', Retrieved January 29th from: http://www.cybersafety.org.nz/kit/policy/template.html

Nicholson, A., 2006, 'Legal perspectives on bullying.' in H.L. McGrath and T. Noble, *Bullying Solutions: Evidence-based Approaches to Bullying in Australian schools*

Ofcom, n.d, '*Executive Summary: Engaging with social networking',* Retrieved February 11th 2009, from: www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

Olweus, D., 1999, Norway, in P. K. Smith, Y. Morita, J. Junger-Tas, D. Olweus, R. Catalano, and P. Slee (Eds.), '*The nature of school bullying: A cross-national perspective'* (pp. 7–27). London: Routledge

Patchin, J. W. and Hinduja, S., 2006, 'Bullies Move beyond the Schoolyard: A Preliminary Look at Cyberbullying', *Youth Violence and Juvenile Justice, 4* (2), 148-169

Pellegrini, A., and Bartini, M., 2000, 'A longitudinal study of bullying, victimization, and peer affiliation during the transition from primary school to middle school', *American Educational Research Journal,* 37(3), 699-725.

Pepler,D. and Craig, W., 2007, '*Binoculars On Bullying: A New Solution to Protect And Connect Children',* Retrieved April 11th, 2009 from: http://www.prevnet.ca/Downloads/tabid/192/Default.aspx

Petersen, L., 2001, 'Anti-bullying programs- Avoiding bullying the bullies', in *Promoting Wellbeing',* AGCA Conference proceedings (pp. 51-60), Brisbane, Australia.

Raskauskas, J., and Stoltz, A. D., 2007, 'Involvement in traditional and electronic bullying among adolescents', *Developmental Psychology, 43*(3), 564-575.

Rigby, K., 2008, '*What is Bullying?'* http://www.kenrigby.net/ (Retrieved April 2nd, 2009)

Ross, D.M., 2002, '*Childhood bullying and teasing: what school personnel, other professionals and parents can do'*, 2nd edition. Alexandria, VA: American Counselling Association.

Sentse, M., Scholte, R. H., Salmivalli, C., and Voeten, M., 2007, 'Person-group dissimilarity in involvement in bullying and its relation with social status', *Journal of Abnormal Child Psychology, 35*, 1009-1019.

Shariff, S., 2005, 'Cyber-dilemmas in the new millennium: Balancing free expression and

student safety in cyber-space' [Special Issue: Schools and courts: Competing rights in the new millennium], *McGill Journal of Education*, 40 (3), 467-487.

Shariff, S., 2006b, 'Cyber-dilemmas: Balancing free expression and learning in the virtual school environment', *International Journal of Learning*, 12 (4), 269-278.

Shariff, S., 2009, '*Confronting Cyber-Bullying: What Schools Need to Know to Control Misconduct and Avoid Legal Consequences'*, Cambridge University Press, New York

Shariff, S., and Gouin, R., 2006, 'Cyber-dilemmas: Gendered hierarchies, new technologies and cyber-safety in schools' *Atlantis - A Women's Studies Journal*, 31 (1), 26-36.

Smith, P.K., 2005, 'Definition, types and prevalence of school bullying and violence', in E. Munthe, E. Solli, E.Y. Arne and E. Roland (eds.), *Taking fear out of schools,* Stavanger: University of Stavangerz: Centre for Behavioural Research. Retrieved January 15th, 2009 from:
http://saf.uis.no/getfile.php/SAF/Til%20nedlast/Taking%20Fear%20out%20of%20Schools.pdf

Smith, P.K. and Brain, P., 2000, 'Bullying in schools: Lessons from two decades of research', *Aggressive Behavior,* 26, 1-9.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., and Tippett, N., 2008, 'Cyberbullying: Its nature and impact in secondary school pupils', *Journal of Child Psychology and Psychiatry, 49*(4), 376-385.

Snider, M., and Borel, K., 2004, 'Stalked by a cyberbully', *Maclean's, 117*(21-22), 76-77. Retrieved May 1st, 2009 from:
http://www.cyberbullying.ca/macleans_May_19_2004.html

Spears, B., Slee, P., Owens, L., and Johnson, B., 2008, '*Behind the Scenes: Insights into the Human Dimension of Covert Bullying: Short Report (December 2008)',* Hawke Research Institute for Sustainable Societies (2009). The Centre for the Analysis of Educational Futures (Flinders University) in partnership with The Coalition to Decrease Bullying, Harassment and Violence in South Australian Schools. Retrieved June 4th, 2009 from:
http://www.deewr.gov.au/Schooling/NationalSafeSchools/Pages/research.aspx

TeacherNet, n.d., '*Safe to Learn: Embedding Anti-bullying Work in Schools',* Retrieved March 3rd, 2009 from:
www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn

Stacey, E., 2009, 'Research into cyberbullying: Student perspectives on cybersafe learning environments', *Informatics in Education - An International Journal, 8, 1*,115-130

Suler, J., 2005, '*Adolescents in cyberspace: The good, the bad, and the ugly',* Retrieved March 3rd, 2009 from: http://www.rider.edu/suler/psycyber/adoles.html

Vandebosch, H. and van Cleemput, K., 2008, 'Defining cyberbullying: a qualitative research into the perceptions of youngsters', *Cyberpsychology & Behaviour,* 11(4):499-503.

Whitlock, J., Powers, J. and Eckenrode, J., 2006, 'The virtual cutting edge: the internet and adolescent self-injury', *Developmental Psychology*, vol. 42, no. 3, pp. 407–17

Willard, N., 2003, 'Off-campus, harmful online student speech', *Journal of School Violence*. 1(2), 65-93

Willard, N., 2004, '*I can't see you – you can't see me: How the use of information and communication technologies can impact responsible behavior',* Retrieved March 4th, 2009 from:
http://www.cyberbully.org/cyberbully/docs/disinhibition.pdf

Willard, N., 2005-2007, '*An educators guide to cyberbullying and cyberthreats'* Retrieved March 4th, 2009 from:
http://www.cyberbully.org/cyberbully/docs/cbcteducator.pdf

Willard, N., 2006, '*Cyberbullying And Cyberthreats: Effectively Managing Internet Use Risks in Schools',* Retrieved March 4th, 2009 from:
http://www.cyberbully.org/cyberbully/docs/cbctpresentation.pdf

Willard, N., 2007a, '*Cyberbullying legislation and school policies: Where are the boundaries of the schoolhouse gate in the new virtual world?',* Retrieved February 4th, 2009 from:
http://www.cyberbully.org/cyberbully/docs/cblegislation.pdf

Wolak, J., Finkelhor, D., Mitchell, K.J. and Ybarra, M.L., 2008, 'Online 'predators' and their victims: Myths, realities, and implications for prevention and treatment', *American Psychologist*, 63, 2,111-128

Ybarra, M. L., and Mitchell, K. J., 2004a, 'Online aggressor/targets, aggressors, and targets: a comparison of associated youth characteristics', *Journal of Child Psychology and Psychiatry and Allied Disciplines,* 45(7), 1308 – 1316.

Ybarra, M. L., and Mitchell, K. J., 2004b, 'Youth engaging in online harassment: Associations with caregiver-child relationships, Internet use, and personal characteristics', *Journal of Adolescence, 27,* 319-336.

Ybarra, M., Mitchell, K., Finkelhor, D., and Wolak, J., 2006, 'Examining characteristics and associated distress related to Internet harassment: Findings from the Second Youth Internet Safety Survey', *Pediatrics,* 118(4): 1169-1177.

Yen J.Y., Ko, C.H., Yen, C.F, Wu, H.Y., and Yang, M., 2007, 'The comorbid psychiatric symptoms of Internet addiction: attention deficit and hyperactivity disorder (ADHD), depression, social phobia, and hostility', *Journal of Adolescent Health,* 41 (1),93-98

Yoo, H.J, Cho, S.C, Ha, J., Yune, S.K,, Kim, S.J,, Hwang, J,, Chung, A,, Sung, Y.H., and Lyoo, I.K., 2004, 'Attention deficit hyperactivity symptoms and internet addiction', *Psychiatry and Clinical Neurosciences*, 58(5):487-94

YouGov, 2006, *MSN Cyberbullying Repor,* Retrieved May 2nd, 2009 from:
http://www.warwickshire.gov.uk/Web/corporate/pages.nsf/Links/1301BDA3D993CD7D8025707D002A3372/$file/44+MSN+cyberbullying+research.pdf

Young, K., n.d., *Centre for Internet Addiction*, http://www.netaddiction.com/