## Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>04</td>
<td>01</td>
</tr>
<tr>
<td>05</td>
<td>1.1</td>
</tr>
<tr>
<td>05</td>
<td>1.2</td>
</tr>
<tr>
<td>06</td>
<td>1.3</td>
</tr>
<tr>
<td>06</td>
<td>1.4</td>
</tr>
<tr>
<td>07</td>
<td>1.5</td>
</tr>
<tr>
<td>08</td>
<td>1.6</td>
</tr>
<tr>
<td>09</td>
<td>1.7</td>
</tr>
<tr>
<td>10</td>
<td>1.8</td>
</tr>
<tr>
<td>10</td>
<td>1.9</td>
</tr>
</tbody>
</table>

| 11   | 02      | Background |
| 12   | 2.1     | Overview |
| 13   | 2.2     | The need for research |

| 14   | 03      | Research objectives |
| 15   | 3.1     | Objectives |
| 16   | 3.2     | Defining the target audiences |

| 17   | 04      | Research methodology |
| 18   | 4.1     | Summary |
| 18   | 4.2     | The sample |
| 19   | 4.3     | Recruitment of respondents |
| 19   | 4.4     | Discussion coverage |
| 20   | 4.5     | Bulletin board questions |
| 21   | 4.6     | Definition of social networking sites and online friends |
| 21   | 4.7     | Notes on reporting |
| 21   | 4.8     | Research timing |

| 23   | 05      | Context and role of social networking services in the lives of children and young people |
| 23   | 5.1     | Context |
| 25   | 5.2     | Role of the internet |

| 29   | 06      | About the sites |
| 30   | 6.1     | Intention of this chapter |
| 30   | 6.2     | How children and young people refer to social networking sites |
| 30   | 6.3     | Perceptions of the role of the sites |
| 31   | 6.4     | How children and young people perceive online vs. Real world interactions |
List of tables and figures

18  Table 1: Sample table
20  Table 2: Bulletin board questions
41  Table 3: Summary of segments
25  Figure 1: Typical websites used by girls according to age
26  Figure 2: Typical websites used by boys according to age
50  Figure 3: The impact of different types of online behaviour
57  Figure 4: Parents perception of who are online ‘friends’
62  Figure 5: How parents and school do and could work together
63  Figure 6: Club Penguin rules
63  Figure 7: Safety messages on social networking services
1.1 Research background and methodology

The Australian Communications and Media Authority (ACMA) manages a national cybersafety education program that includes:

> undertaking targeted information and awareness-raising campaigns, activities and programs;
> developing cybersafety education materials for use in schools and at home; and
> researching current trends in cybersafety.

Work is currently underway to review and update the current set of cybersafety products and programs aimed at children, young people and their parents.

Research was commissioned to enhance existing insights into the role online interaction currently plays in the lives of Australian children and young people. Other issues explored by the research included how children’s and young people’s behaviour is influenced by their peers and families, as well as the impact of recent and emerging online activities and technologies, including social networking services.

A combined qualitative and quantitative approach was adopted. This report outlines the results of the qualitative component only. The qualitative methodology consisted of:

> two bulletin boards and four discussion groups with 13 to 17-year-olds;
> eight in-home triad interviews with eight to 12-year-olds; and
> a combination of in-depth interviews and discussion groups with parents of eight to 17-year-olds.

The remainder of this executive summary presents the key findings of the qualitative research.

1.2 Key findings: Context and role of social networking services in the lives of children and young people

The internet is a regular part of everyday lives of children and young people aged eight to 17 years, and is used regularly within both school and home environments.

Children and young people aged eight to 17 use the internet to find information, for academic purposes and social networking. Exposure to the internet and social networking services increases with age, starting predominantly with game-related websites at younger ages, leading into regular and proficient use of social networking services from high school age upwards (12+ years).

At a young age (eight to 10 years), the internet is regarded primarily as a source of entertainment, and websites used are often closed game websites such as MiniClip (games for one player). From the age of about 10, interaction occurs on open game websites (multiplayer games) like Club Penguin, and, particularly for boys, role playing games such as Runescape and World of Warcraft.

On entering high school (from 12 years on) the social lives of boys and girls change, with their interests and friendship circles increasing. These changes are reflected in their online environment. From this age, young people tend to have accounts and be regular users of social networking sites and services such as MSN, Bebo and MySpace. For this age group, the importance and role of the social networking services is to provide an arena for self-expression, ‘fitting in’, chatting with people they know and also people they do not necessarily know offline.
For older teenagers, social networking services are more often used as a platform to meet and chat to members of the opposite gender and (for boys) to entertain themselves and others through practical joke playing.

Parents tend to have the perspective that social networking services are an integral part of growing up. Parents control and monitor their children’s internet access more strictly at the primary school age.

1.3
Key findings: About the social networking services

Among the research participants, the term ‘social networking’ was largely understood but not commonly used, and particular websites were referred to collectively as different things, without any consistent terminology. Some were called chatrooms, some forums and, more commonly amongst parents, diary websites. Ultimately the most common way of talking about and referring to the different websites was to use their brand names.

Maybe because the use of social networking websites begins through multi-player games websites such as Club Penguin or Runescape, there is some indication that interactions with other people on such websites are also perceived as just ‘part of a game’. When online profiles are created, time and effort is given to making them highly ‘expressive’ through skins and other personalisation, and this could be considered similar to creating an avatar in role playing games.

Parents held the view that social networking services were often seen by their children as part of a ‘fantasy land’ where children and young people were either unaware or could easily believe that their interactions did not have real world consequences.

1.4
Key findings: Perceptions of risk and cybersafety

Perceptions of risk by children and young people may be divided into two areas: general online risks and risks specifically associated with social networking services.

The general risks associated with online behaviour include computer viruses from downloaded material and accidental exposure to graphic or explicit material. Risks identified as specific to social networking include being contacted by a predator, encountering undesirable behaviour (often via webcams), unwanted dissemination of personal information and cyberbullying.

Of the age groups consulted, children and young teenagers were more inclined to identify contact with a predator as a risk arising from online conduct. This result appeared to be an outcome of parents identifying and discussing this risk with younger children, as well as school cybersafety educational programs focusing on it. In contrast, older teenagers were more sceptical that there was any real risk of being targeted by a predator, largely due to their not having encountered such a problem personally during years of using social networking websites.

Girls perceived there were risks associated with being the target of lewd or indecent behaviour (often via webcam) or having their personal material disseminated to unintended recipients. Again, this perception arose from actual experience (or a friend’s experience) of such behaviour.
Cyberbullying was very much seen as a risk associated with social networking websites such as the profile websites Bebo and MySpace, and thus more of a concern for teenagers. Of this group, girls tended to see the risk as more relevant and immediate, with girls believing they were more likely to experience, or had already experienced cyberbullying. For older girls, bullying was more related to personal attacks on their appearance, comments about their friends/family or personal information about themselves, than name-calling only. By contrast, boys claimed to have little exposure to cyberbullying, and accordingly did not perceive it to be a real risk.

However, parents believed that offline risks present in children’s lives, such as actual face-to-face bullying, exceeded any potential online danger.

1.5 Key findings: Segmenting teenagers

From the qualitative findings it was possible to tentatively segment teenagers into a number of key groups according to their claimed online behaviour. (It should be noted that no attempt was made to segment young children because of the methodology used to survey them).

For teenagers, the segments that emerged are described below:

Active Risk-takers are characteristically outgoing and confident. Members of this segment are more likely to have met someone face-to-face after meeting them online first, used webcams inappropriately and maintain public profile pages on social networking services. Active Risk-takers believe their safety is their own responsibility, perceiving themselves as highly knowledgeable about online risks. Importantly, members of this segment believe that they know the risks and take active steps to mitigate them. This group may have experienced cyberbullying through interactions with friends, who are friends both on and offline, or with strangers who they have accepted as friends.

Responsible Risk-takers are similar to Active Risk-takers, differing in that they take risks online but only to a certain point. They would be likely to have friends on social networking services that they do not know personally offline, would accept friend invitations from people they do not know and have experienced cyberbullying. Members of this segment would take steps to limit the risks they face online; for example, they would chat to strangers online, but not meet them face-to-face, use a webcam with a stranger but only when the stranger switched on their webcam first, or upload personal information and photos but limit the specificity of the details.

The Vulnerably Influenced are less active in their use of social networking services and generally quieter in nature. Members of this segment use social networking services to ‘fit in’ and often claim they take risks online, but in reality rarely do so. Despite their inactivity, this segment has the potential to be influenced and take risks, especially as they are likely to be less aware of all the risks and the consequences. They are also less likely to be aware of what they can do to mitigate risks.

Specialist Seekers tend to use social networking services in relation to special interests or hobbies rather than as a means of expanding their general social networks. Their risk taking tends to take the form of seeking out and interacting with people they do not know offline but claim to have similar interests to them.

Claimed Conformists maintain that they conform to online safety rules they have been taught and take few risks. Such conformity is displayed by only having a private profile page, not accepting friend invitations from strangers and never uploading personal information about themselves. Generally, this segment is younger in age. Moreover, parents were more likely to claim that their children exhibited such behaviour than were the children themselves.
1.6
Key findings: Content, contact and privacy risk behaviours

Research in the European Union identified three key areas of concern in relation to cybersafety risks for children and young people. ACMA wanted to test how these risks were perceived in the Australian context.

Content
When asked about what type of content they had come across online that they didn’t like, children and young people identified violent, pornographic or other sexual material. It was believed that such content could be accessed by pop-ups, downloads, file sharing, or Google images. For children and young people, the perceived consequences of accessing such risky content included contracting computer viruses, getting into trouble with parents, or exposure to unpleasant or explicit material.

Such material may be found accidentally, or sought purposefully to indulge curiosity or sought to share with friends. Males were more inclined than females to seek graphic or violent material for their own personal curiosity and to share with friends.

Contact
Whilst predator risks are forefront in children and young people’s minds, they are not actively concerned about other risks that may arise from online contact. Those of primary school (8 to 12 years) age are often content with their immediate friendship circles and do not actively seek or desire contact with people they do not know. In comparison, the lifestyle, friendships and curiosity of 13 to 17-year-olds expands at a faster rate through high school years and the fun and freedom that comes with growing up and experimenting tends to outweigh any perceived risks.

Types of potentially risky behaviour that may arise through contact made online included accepting friend invites from people not known offline (especially 15 to 17-year-olds), use of a webcam, and meeting up with people offline that they first met online. The extent to which those surveyed identified they would engage in such behaviour varied according to age and the segment that they belonged to.

Cyberbullying was also identified as a risky behaviour falling into the ‘contact’ category.

Privacy
Often young people choose to be open and expressive. The option of protecting their privacy online often falls by the wayside in favour of wanting to stand out to others online. Young people may attempt to stand out through expressive profile pages, welcoming attention from the opposite sex, and making or accepting friend requests from those with similar interests. Purposeful divulgence of personal details such as passwords was commonplace. Sometimes personal information was divulged without an understanding of the potential consequences of disclosure (for example, posting information about going on holiday and not realising that this could give an unintended recipient information about their whereabouts).
1.7
Key findings: Management of online risks

The extent to which young people manage online risks depends on whether risk is perceived to be present. There are four main ways in which children and young people manage risk online:

> abiding by the rules or advice given to them;
> using commonsense;
> learning from experience; and
> resilience.

Abiding by the rules and applying commonsense are relatively easy strategies, which tend to be used by the eight to 10-year-olds. Methods this age group might use to mitigate risk would be giving only parents their password, scanning downloadable files, and reporting someone who is behaving inappropriately or offensive material they come across online.

Beginning from a young age, children apply commonsense, begin to learn from experience, and develop resilience. These behaviours or strategies are acquired as children become more adept at managing their online experiences. Often, they learn to modify behaviour after encountering some unsought experiences online. For example, they may make their profile page private after receiving unwanted comments on their public profile page, or avoid downloading suspect files after getting a virus. Exposure over time to unsought experiences can result in an individual learning how best to handle such situations.

Whilst most young people believe that they are primarily responsible for keeping themselves safe online, many also believe website providers should play a part in making sure their users are safe. For example, privacy controls are considered important in providing children and young people with the choice to protect themselves, regardless of whether they actually use them.
1.8
Key findings: The role of parents

Parents openly admitted that they were likely to be less knowledgeable about their children’s online safety as they should be, or in fact as their children are. Similarly, whilst they made efforts to inform and advise their children about potential risks and how to mitigate them, they were not fully aware of the extent of these risks or when best to discuss them with their children.

When children were young (eight to 10-year-olds), parents focused their discussions with them on the risks of viruses and unsuitable content. When children began to use social networking websites, at around 11 years, parents discussed not giving personal details to others and avoiding contact with those they did not know. Parents then reiterate this risk as children get older.

Most parents claimed, in respect of their own children, that it was unlikely that they would have contact with people they did not already know offline or reveal their personal details online. However, they acknowledged that it was more likely that their children might access inappropriate material.

There appeared to be varying degrees of monitoring and control placed on eight to 17-year-olds. Parental styles for managing their children’s online behaviour ranged from relying solely on trust to being very controlling. Parents’ level of knowledge about what children were doing online also varied widely. Broadly speaking, younger children were watched a little more closely and many parents had initiated placing the computer in a central, open part of the household. However, for older children, parents were relatively trusting and often relied at most on filters and occasional monitoring.

1.9
Key findings: Communication of online safety messages

Online safety messages are communicated through three main channels:

> schools (in the most part);
> parents; and
> websites.

While schools are considered successful in disseminating the basic safety messages, often communications and the delivery fail to engage beyond this. Parents tend to re-enforce the basic internet safety messages with a stronger focus on the issue of predators rather than the broader range of safety issues. Both schools and parents currently appear to work in isolation in informing children about cybersafety, although parents did show interest in a more collaborative approach with schools. It was found that the safety messages on the social networking websites were often ignored or missed. Those that were more likely to be noticed and acknowledged were those that displayed their safety rules/agreement explicitly on the initial log-in page, for example Club Penguin and Runescape.
02
Background
2.1 Overview

The Australian Communications and Media Authority (ACMA) is a statutory authority within the federal government portfolio of Broadband, Communications and the Digital Economy. ACMA is responsible for the regulation of broadcasting, the internet, radiocommunications and telecommunications.

ACMA has a role in advising parents and carers about the supervision and control of children’s access to the internet, as well as conducting and coordinating educational programs about internet content and internet carriage services. The Cybersafety Programs and Cybersafety Outreach Sections within ACMA manage a national cybersafety program to help parents and children manage online risks. This includes:

- researching current trends in cybersafety;
- undertaking targeted information and awareness raising campaigns and activities; and
- developing cybersafety education materials for use in schools.

ACMA recognises that the internet is a valuable resource that facilitates ‘identity building, creative activities, and managing interpersonal relationships’ among children and young people and is ‘an important resource for formal and informal learning.’ Cybersafety publications therefore aim to present positive messages about the internet, while embedding protective behaviours among children, young people, parents and teachers to enable them to manage cybersafety issues.

Research in the European Union has identified three key areas of concern in relation to cybersafety risks for children and young people. These are:

- ‘content’ risks: including exposure to illegal content, exposure to harmful content, encountering sexual/violent/racist/hate material, misinformation, (problematic) user generated content, challenging content (for example, suicide, anorexia and drugs);
- ‘contact’ risks: including contact with strangers and cyberbullying; and
- ‘privacy’ risks: including giving out personal information, invasion of privacy and hacking.

ACMA is seeking to update its cybersafety resources to ensure they address current issues associated with online behaviour. A key challenge for ACMA is the time sensitivity of research on this topic, given the rapid pace of change in this area as a result of technological developments and trends in behaviour among the key audiences.

Attitudes and behaviour relating to user-generated content, including social networking services such as MySpace and Facebook, are an area of interest for ACMA because of the new ways in which they enable young people to express themselves and interact online.

---
2 LSE (2007), EU Kids Online: What do we know about Children’s use of online technologies? A report on data availability and research gaps in Europe, p. 7
2.2 The need for research

ACMA commissioned market research to explore current perceptions of online risks and opportunities among children and young people and their parents in Australia. This research will assist ACMA in updating its suite of cybersafety materials and programs.

Exploratory qualitative research was required to provide detailed information about the attitudes and behaviour of children and young people in relation to a broad range of topics including social networking online and other technology-driven trends. While an evaluation of ACMA cybersafety materials was not the focus of the research, use of these materials as stimulus in group discussions helped to identify useful principles for future communications.

A quantitative stage of research was subsequently undertaken, and is reported under separate cover.
Research objectives
3.1 Objectives

The objective of the project overall was to generate up-to-date insights on the role online interaction currently plays in the lives of Australian children and young people, and how their peers and families influence their behaviour. A key element within this was to explore the impact of recent and emerging online activities and technologies, including social networking services.

The objectives of the qualitative phase were to explore:

> children and young people’s perceptions of social networking services:
  > attitudes and perceptions of social networking services and the role of these in their lives;
  > perceptions of social networking activities within the context of their everyday lives;
  > how they perceive cybersafety, particularly in relation to services that have become popular relatively recently, such as social networking and others involving user generated content;
  > perceptions of online risks in general to people their age;
  > perceptions of the risks involved in online social relationships;
  > perceptions of the potential impact of social networking on cyberbullying.

> children and young people’s online behaviours and attitudes that may lead to or involve ‘contact’, ‘content’ or ‘privacy’ risks:
  > perceptions of the potential for unpleasant experiences when using social networking services;
  > specific ‘content’, ‘contact’ and ‘privacy’ related concerns;
  > the perceived importance of privacy controls when using social networking services;
  > reasons for engaging in high risk behaviours online;
  > the impact of online skill/experience and engaging in high risk behaviours;
  > whether the presence of peers influences behaviour;
  > how offline and online risk-taking behaviours compare.

> children and young people’s self-management of online risk, including through protective behaviours and resilience:
  > strategies in place to manage or mitigate risks;
  > children and young people’s response to and awareness of online safety messages;
  > information resources currently used to manage risk;
  > best practice in terms of messages and communication style and channels to communicate online safety.

> the role of parents in children and young people’s experiences and use of social networking services:
  > ease of communication between children and their parents, including the extent to which they speak a common language on the issue;
  > how they work together to manage online risks;
> the influence of older siblings and peers on experience and use of social networking services.

The objectives for the quantitative stage of research were to:

> establish the extent to which the main qualitative findings are present in the population;
> identify those at highest risk of exposure to online threats;
> establish the factors that predict online risk-taking behaviours;
> determine awareness, access and usage of social networking services;
> examine the role of mediating factors in reducing children’s online interaction risks.

### 3.2 Defining the target audiences

The target audiences for the research were defined as follows:

> children and young people aged eight to 17 who use the internet, including:
  > those who have actively used social networking services in order to explore the issues relating to risks associated with using these services;
  > those who have/have not engaged in risk-taking behaviours in order to understand the reasons for these behaviours and to identify the characteristics of those who are most likely to adopt them.

> parents or carers of children and young people aged eight to 17, including:
  > a mix of parents with different levels of internet literacy, to explore the impact of this variable on their perceptions of online risks faced by their children; and
  > some who are aware that their children have used social networking services, to explore their perceptions of this type of activity.
04
Research methodology
4.1 Summary

The program of qualitative research consisted of:

> four focus group discussions with young people aged 13 to 17 years;
> two focus group discussions with parents of this age group;
> eight ‘friendship’ triads with children aged eight to 12 years, followed by paired in-depth interviews with their parents; and
> two bulletin boards with teenagers aged 13 to 17 years.

All group discussions consisted of eight respondents and were of 1.5 hours duration. Triads consisted of three friends and were conducted at home where children could demonstrate their computer use. Triads were of approximately one hour duration.

The subsequent paired in-depth interviews were conducted with one parent of two of the children involved the triad. These interviews were of approximately one hour duration.

The two bulletin boards were run over a 10-day period. One bulletin board consisted of participants in school grades 8 and 9 (aged 13 to 15 years), and the other consisted of participants in school grades 10 and 11 (aged 15 to 17 years). Twenty-one participants took part overall, with three quarters of these participants also attending a focus group discussion. The bulletin boards were operational three to four days before group discussions and for five to six days after. Questions were posted daily over the 10-day period. Additional questions were also asked by the moderator to individuals to gain further depth to specific answers and participants could also comment on the responses of others.

4.2 The sample

Table 1: Sample table

<table>
<thead>
<tr>
<th>Session</th>
<th>Type</th>
<th>Age/Audience</th>
<th>Gender</th>
<th>Location</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In-home friendship triads, plus two parents per triad</td>
<td>8–9 (primary school year 3)</td>
<td></td>
<td>Sydney</td>
<td>NSW</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>9–10 (primary school year 4)</td>
<td></td>
<td>Brisbane</td>
<td>QLD</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>10–11 (primary school year 5)</td>
<td>Mixed</td>
<td>Dubbo</td>
<td>NSW</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>11–12 (primary school year 6)</td>
<td></td>
<td>Melbourne</td>
<td>VIC</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>12–13 (high school years 8 and 9)</td>
<td>Males</td>
<td>Melbourne</td>
<td>VIC</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>13–15 (high school years 8 and 9)</td>
<td>Females</td>
<td>Dubbo</td>
<td>NSW</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>16–17 (high school years 10 and 11)</td>
<td>Males</td>
<td>Brisbane</td>
<td>QLD</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>16–17 (high school years 10 and 11)</td>
<td>Females</td>
<td>Sydney</td>
<td>NSW</td>
</tr>
<tr>
<td>9</td>
<td>Focus groups plus younger-teen online ‘bulletin board’</td>
<td>13–15 (high school years 8 and 9)</td>
<td>Males</td>
<td>Brisbane</td>
<td>QLD</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>13–15 (high school years 8 and 9)</td>
<td>Females</td>
<td>Dubbo</td>
<td>NSW</td>
</tr>
<tr>
<td>11</td>
<td>Focus groups plus older-teen online ‘bulletin board’</td>
<td>16–17 (high school years 10 and 11)</td>
<td>Males</td>
<td>Brisbane</td>
<td>QLD</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>16–17 (high school years 10 and 11)</td>
<td>Females</td>
<td>Sydney</td>
<td>NSW</td>
</tr>
<tr>
<td>13</td>
<td>Focus groups</td>
<td>Parents of high school aged children</td>
<td>Mixed</td>
<td>Melbourne</td>
<td>VIC</td>
</tr>
</tbody>
</table>
4.3 Recruitment of respondents

Recruitment for all audiences was from commercial lists by specialist Interviewer Quality Control Australia (IQCA)-accredited recruitment companies. A recruitment screener was used for all groups. Unless specified, all of the following questions were asked of potential participants:

- presence of internet access at home;
- frequency of internet use by child for non-school related activities;
- child’s use of social networking services;
- likelihood of undertaking risky online activities (teenagers only);
- child’s school year;
- parent’s perceived awareness of child’s online activities (parents only).

The full recruitment criteria can be found in Appendix A.

4.4 Discussion coverage

A semi-structured discussion guide was used, which allowed the respondents themselves to dictate the flow of discussion with guidance from the moderator, rather than the questions being administered in the question-response format common in quantitative research.

For the group discussions with those aged 13 to 17 years, the discussion guide included the following areas:

- online behaviour;
- social networking websites and services;
- online relationships (contact);
- sharing of information (privacy);
- online material (content);
- online safety; and
- reactions to existing cybersafety materials.

The discussion guide with parents in both groups and paired in-depth interviews covered the same areas, with the emphasis being on their children’s behaviour. Instead of discussing social networking websites and services, the discussion guide for the triads with eight to 12-year-olds included the child showing researchers which websites and other internet services they normally use in a typical online session, and did not include a prompted discussion on privacy and contact issues.

The discussion guides (Appendix B) were approved by ACMA prior to use.
### Bulletin board questions

#### Table 2: Bulletin board questions

<table>
<thead>
<tr>
<th>Topic</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>About You</td>
<td>&gt; What can you tell me about you and your family?</td>
</tr>
<tr>
<td>Online Activity</td>
<td>&gt; Which websites do you like and why?</td>
</tr>
<tr>
<td>Chatting Online</td>
<td>&gt; Which websites are best for chatting to people and why?</td>
</tr>
<tr>
<td>Chatting &amp; Posting Online</td>
<td>&gt; What do you chat about online?</td>
</tr>
<tr>
<td></td>
<td>&gt; Have you ever posted anything online? If so what?</td>
</tr>
</tbody>
</table>
| Online Risks                       | > What risks are there going on websites like Bebo, Facebook and MSN?  
> Have you or anybody you know done anything online which could be considered risky? *(only asked of 16–17 yr olds)*  
> Have you knowingly or accidentally accessed something that you shouldn’t  
> Can you give examples or any experiences of the risks you could get on each website (Bebo, Facebook and MSN)? *(only asked of 13–15 yr olds)*                                                                                                                                 |
| Online Risks                       | > Who do you think knows the most about what is risky online and what isn’t?  
Is it your parents? You? Your friends? The website provider? Your school? Someone else?  
> Why do you think they know more than the others?                                                                                                                                                                                                                                                                                                   |
| Website Feedback                   | > What do you think of the name of this website?  
> If you had to come up with a different website name what would it be?  
> What sort of things would you like to see on an online safety website?  
> Should online safety information be on a separate website or part of a website you already visit? Why?                                                                                                                                                                                                                                           |
| Chat Rooms, Forums & Message Boards| > Can you tell us about your experiences of …  
> … chat rooms? … forums? … message boards?  
> What do you like/dislike about each?  
> How safe do you feel each of these are? Why?  
> If you haven’t used any of these—why?                                                                                                                                                                                                                                                                                                           |
4.6 Definition of social networking services and online friends

A social networking service (SNS) can be defined as an online social network for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others. As a member of a social networking service, individuals can ‘chat’ with each other via messaging, email, video or voice chat, share photos and videos and post comments in online forums, blogs or discussion groups. Profiles may contain personal information such as real life photos and descriptive comments about the member.

The main types of social networking services are those which contain directories of some categories (such as former classmates) and ways of connecting with friends (usually with self-description pages). In general, each social networking service has a different focus and offers differing levels of access and protection for users. Examples of popular social networking services are used as examples in this research are Bebo, Club Penguin, Facebook, MSN Messenger and MySpace.

In the online environment, the term ‘friend’ can have a different meaning to its common usage in an offline setting. Users of online social networking services can invite and accept ‘friends’ without initially knowing the person or subsequently forming a relationship with them. For the purposes of this report, unknown online friends may also be referred to as ‘strangers’.3

4.7 Notes on reporting

Qualitative research deals with relatively small numbers of consumers, and explores their in-depth motivations, attitudes, feelings and behaviour. The exchange of views and experiences among participants is relatively free-flowing and open, and as a result, often provides very rich data that can be broadly representative of the population at large. The opinions of respondents are indicative of their immediate perception of issues. However, the findings are not based on statistical analysis, but on the experience and expertise of the researchers in analysing the discussions and are interpretive in nature.

Findings and observations from the online bulletin boards have been included throughout this document, particularly to:

> clarify some of the issues raised in the focus group discussions; and
> provide unique insight into the development of segments of users.

The discussions with parents assisted in interpreting many of the findings regarding children and young people. Where findings were specific to parents only, these have been indicated; where findings were consistent between both parents and children, no distinction is drawn.

Quotes from respondents have been provided verbatim. These are presented in italics and are indicated by quotation marks. For example,

“Each quote is presented verbatim and in italics.”

4.8 Research timing

The qualitative research was conducted between 7 and 17 June 2008.

---

3 The qualitative research found that it was commonplace that, if the friend is unknown, then they can also be referred to as a ‘random’. This term was not used in the quantitative questionnaire.
Detailed findings
Context and role of social networking services in the lives of children and young people
5.1 Context

The internet is a regular part of the everyday lives of children and young people, who have grown up with this technology as part of their lives. Children begin to use the internet in primary school and are taught to make regular use of it at school during their high school years, with an expectation that the medium will be used regularly for homework and assignments. Some schools provide laptops to students in high school.

At the same time, children and young people have grown up using the internet as a primary source of information for interests and hobbies. For example, young people regularly use the internet to check sport training times and games timetables, or to research different various personal interests, such as music, movies, and products they want to buy. Children and young people have also grown up at a time when the internet is used as a key communication and information tool for their parents both in a work and personal capacity.

Given the pervasiveness of the internet, it is natural for children and young people to use the internet for socialising as well. The internet is now used by this generation for socialising as much as the telephone once was. However, the internet offers additional benefits to the telephone, including:

> being able to talk to several friends at once;
  
  “It is easier to talk on MSN than make phone calls.”

  “I can keep up with friends that I do not go to the same school as now.”

> being able to socialise while doing other activities such as homework; and
  
  “I’m not on MSN all the time … I have it on in the background while I’m doing homework and stuff.”

> providing a means of gaining insight into people with whom young people may not interact easily in person.
  
  “You get to know people by looking at their profile.”

Broadly, the importance of the internet in the lives of children and young people increases not only as they grow older, but also with the time they spend using the technology.

While every child is different in terms of how much time they claim to spend on the internet, it is possible to identify a broad pattern from the research conducted. Children aged eight to nine years had little exposure to the internet at school and predominantly used the medium at home for entertainment. At this age, children have shorter attention spans and move quickly from one activity to the next. Use of the internet is not a priority; instead it is simply a means of being entertained for a short period of time.

Children aged 10 to 12 years appeared to have greater exposure and familiarity with the internet as a source of information as well as of entertainment. These children were beginning to use the internet to research areas of interest, but the internet was not yet an integral part of their lives. Most parents of children this age claimed to restrict the time spent on the internet and to encourage offline activities.

Use of the internet becomes a more prominent part of a child’s life once they begin high school. Younger teenagers (aged 13 to 15) are expected to make almost daily use of the internet for school activities. It is in the young teenage years that the internet also begins to have a role in their social environment. For example, young teenagers increasingly begin to use the internet as a means to converse with friends, swap stories or chat about their daily lives, and talk about areas of interest such as good movies to see. Some may use instant messaging services, such as MSN, to arrange to meet up on the weekend.
One of the main drivers for increased internet use at this age is the transition from primary school to high school. It is at this time that their social world changes, from the small circle of the friends they have at primary school to an expanded circle of high school friends. The internet becomes a means of keeping in touch with friends, both those they no longer go to school with, and those that they do. As they are also frequently using the internet for school activities, the time spent on online activities compared to offline activities increases. As the internet is an important medium for school life, parents do not tend to restrict the time spent online as much as they do with younger children. The importance of the internet to a young teenager’s life becomes less able to be monitored or controlled by parents.

Older teenagers (aged 15 to 17) are required to be adept at using the internet as an information source and means of communication for school. Many of these teenagers claimed that they had few, if any, parental restrictions on time spent online and could therefore pursue interests outside of school activities as much as they individually wished. The importance of the internet to the everyday lives of older teenagers, including their social lives, varies considerably across the children surveyed. For some it has a central role, whereas for others it is merely an additional means of talking to friends.

Broadly, however, older teenagers are beginning to become more interested in socialising in person than online. It is at this age that parental controls on face-to-face socialising are more lenient, providing older teenagers with an increased capacity to socialise in person. Correspondingly, it is also at this age that the likelihood for face-to-face meetings from online relationships developed through social networking services increases considerably.

5.2 Role of the internet

The role of social networking services in the lives of children varies with gender and age.

Gender

As shown in Figure 1 below, girls start using the internet as a source of entertainment primarily through game playing, but by high school are using the internet predominantly for socialising. Young girls (aged eight to 10) use closed game websites, such as MiniClip and Neopets, for entertainment. At this age some may also start using multi-player games websites, such as Club Penguin, where they can interact with other players. More frequent use of Club Penguin started when girls reached 10 to 12 years, and girls this age claimed to make arrangements on multi-player websites such as Club Penguin to meet friends offline after school. While still a means of entertainment, the multi-player websites begin to be seen as a means of interacting with others.

Figure 1: Typical websites used by girls according to age
Once girls reach high school, the internet is no longer solely a source of entertainment. Based on the amount of time spent on particular websites, the use of social networking websites appears to increase dramatically. While the websites can be used for entertainment, in that girls like to look at the profiles of others, the internet begins to have a key role in maintaining and expanding social networks. Teenage girls in the group discussions claimed to spend a large portion of online time chatting on MSN messenger. In addition, other significant portions of online time were spent on Bebo, MySpace and YouTube. The majority claimed not to use Facebook, as the website was considered to be used more by older teenagers.

In contrast to girls, the role of the internet for both younger and teenage boys is very much one of entertainment. Boys are more likely to use the internet to pursue interests and hobbies, such as participating in competitions to pick winners in their favourite sporting league. Use of the internet for this type of entertainment appears to continue into the teenage years for boys much longer than it does for girls. As shown in Figure 2 below, boys aged eight to 10 years, similarly to girls of this age, use closed game websites such as MiniClip and Neopets, along with multi-player game websites, such as Club Penguin.

**Figure 2: Typical websites used by boys according to age**

<table>
<thead>
<tr>
<th>Age</th>
<th>8-10</th>
<th>10-12</th>
<th>12-14</th>
<th>15-17</th>
<th>16+</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Closed game sites, e.g. MiniClip</td>
<td>Closed game sites, e.g. RuneScape, World of Warcraft, Habbo</td>
<td>MSN, MySpace, YouTube, Bebo, Games, Interests / Hobbies</td>
<td>MSN, MySpace, YouTube, Bebo, Interests / Hobbies</td>
<td>Facebook added into repertoire for some adults</td>
</tr>
<tr>
<td></td>
<td>Open game sites, e.g. Club Penguin</td>
<td>Interests / Hobbies, e.g. how to build model trains / rollercoaster, AFL Dream Team Comp</td>
<td></td>
<td></td>
<td>Generally seen as a more ‘adult’ site</td>
</tr>
<tr>
<td></td>
<td>Interests / Hobbies, e.g. participating in competitions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

However, while girls aged 10 to 12 start to use the internet for communication, boys aged 10 to 12 continue to use the internet primarily for entertainment. Boys are more likely to expand their use of multi-player game websites beyond that of Club Penguin at this age, including to games websites such as RuneScape, World of Warcraft and Habbo. Boys of this age in the triad discussions were also more likely to use instant messaging services, such as MSN Messenger, than were girls of this age.

As with girls, social networking websites and services began to assume a greater role in the lives of boys once they reached high school. MSN Messenger was the most prominent service, followed by social networking websites MySpace, YouTube and Bebo. However, boys in the group discussions were more likely to claim continued use of games and hobbies websites than were teenage girls. As with girls, Facebook was generally perceived to be a website for adults, with few boys using it.

---

1 While Habbo may be considered more of a social networking site by definition, as young people can interact with each other, it was perceived by many of those who were familiar with the site as having more of a game-like quality. This was due to the site being a virtual world, where young people created avatars to interact with others.
Age
From the perspective of age rather than gender, the internet is largely a source of entertainment for young children (aged eight to 10 years). Games websites, such as MiniClip, offer a large range of games for children to choose from, providing a range of entertainment options. Through these games websites, children are introduced to multi-player games websites, such as Club Penguin. Children choose what their character looks like and must do activities and tasks to earn points or currency to use in the game. In addition, although not acknowledged by children themselves, these websites also improve computer skills.

The role of the websites beyond purely entertainment begins between the ages of 10 to 12. At this age, girls identify Club Penguin as having a role in socialising with friends, as online activity begins to be about talking to others. They will arrange to meet each other in online rooms. At this age, they also begin to interact with other ‘penguins’ they do not know personally by talking to each other in the common spaces as well as visiting their ‘igloos’. It is also at this age that girls begin to express themselves over the internet, as they start to experiment with creating a character for themselves via their penguin image.

In contrast, while boys are also beginning to use multi-player game websites, the emphasis of online activity is more about competition and pursuing special interests and hobbies than socialising with others. For boys aged 10 to 12 years, the multi-player game websites were enjoyed because of the competition and the ability to learn new skills. Boys also used these websites to ask questions and compete in areas of special interest or hobbies in online clubs or forums.

The use of social networking services increases dramatically once children reach high school age (aged 12 and over). Instant messaging becomes a major feature of online time for both genders at the beginning of high school and continues throughout teenage years. MSN Messenger in particular is used much the same way in which friends used the telephone to speak after school 10 to 15 years ago, and teenagers value the instant communication with friends that this service provides.

User-generated social networking services are generally added to the online repertoire around 13 to 17 years of age. For both genders, these services play a number of roles:

- entertainment;
- visually exploring areas of interest and hobbies (specifically YouTube);
- exploring and expressing different aspects of their personality;
- learning about other people by reading their profile (both those they know and those they do not);
- being able to ‘talk’ to those that they might be too shy to speak to in person;
- keeping up-to-date with latest news from non-school friends, and trends in music, fashion, and films; and
- expanding their social network.

User-generated social networking services in particular play a large role in teenagers’ efforts to conform to group norms and culture, and develop and maintain social currency. These services allow teenagers to keep up with topics of conversations at school and to feel they are part of mainstream teenage culture, as there is a general perception that all teenagers are on at least one of the social networking services.
Parents also considered this characteristic as one of the key reasons for allowing their children to use such services. The quotes below illustrate this:

"When she turned 14, we signed up to MySpace together. All her friends are on MySpace." (Parent of 10 to 11-year-old boy and teenage girl)

"I couldn’t let her be the only one not on MySpace." (Parent of teenage girl)

The way in which social networking services are important to teenagers varies across genders. Girls tend to use the services to interact with others. Girls aged 13 to 17 years are more likely to value the services as they are a means of:

> expressing themselves;
> overcoming ‘shyness’ by being able to talk to those they would not otherwise;
> ensuring they are ‘up-to-date’;
> fitting in with everyone else;
> meeting and talking to boys online (more common with 16 to 17-year-olds); and
> meeting and talking to other girls.

In contrast, boys aged 13 to 17 years tend to use social networking services more for entertainment than for conversation, and socialising with a range of others. For teenage boys, social networking services have two key roles:

> meeting and talking to girls (claimed by all teenage boys); and
> being entertained through playing games, watching videos, teasing or playing practical jokes on friends.

Older boys especially claimed to be unlikely to interact with other boys that they did not know on social networking services, except when interacting regarding special interests and hobbies. In contrast, girls are more at ease with interacting with other girls they do not know personally.
06
About the services
6.1
Intention of this chapter

The purpose of this chapter is to examine the perceptions of children and young people regarding social networking services. All data described is based on the perceptions of children and young people involved in the study.

6.2
How children and young people refer to social networking services

How the different websites were referred to collectively as a group varied considerably across the sample. While the terminology of ‘social networking websites’ was largely understood, it was not commonly used.

Other names for the websites provoked a number of different reactions. The terminology ‘chatrooms’ had very different meanings for respondents across the sample. Some saw it as old-fashioned and not applicable to any of the websites in popular use today, others classified instant messaging services (such as MSN Messenger) as chatrooms. Still others perceived the term could apply specifically to websites such as Bebo and MySpace.

The term ‘forums’ held both negative and positive connotations and was not considered a collective name to describe social networking services. It was negatively perceived as having sexual connotations, especially when associated with older people. In contrast, others positively associated the name with websites on special interests or hobbies where interesting pieces of advice could be asked for and questions answered.

The phrase ‘diary websites’ was used by some parents to describe websites where a profile could be created. However, no children or young people identified such websites with this name.

This result suggests that no one name will be perceived to encompass all the relevant services, which are generally known by their brand names.

6.3
Perceptions of the role of the services

Part of the reason it is difficult to find a common name that encompasses all social networking websites or services is because the various services seem to have different roles in the lives of the young people using them.

Games websites are seen as very much about entertainment. These websites are considered largely impersonal and part of a fantasy land that the child or young person enters. As children grow older and begin to use YouTube, the element of entertainment continues to be an important reason for use. Use of YouTube is predominantly about watching videos of others, and is almost considered similar to watching television. The information on the website is perceived as largely impersonal, as its role is to entertain. Even those young people who post content on YouTube are more likely to see that content as designed to entertain.

As young people begin to use other services such as Bebo and MySpace, the element of entertainment is maintained to some extent. As the exchange of information is usually not immediate, the websites are more about ‘seeing’ what others have done or are doing than about direct interaction. At the same time, these websites offer the opportunity for children and young people to express themselves by the profiles they design and post. Therefore while there is an element of the websites being personal, they are still largely viewed as entertainment and are impersonal.
Special interest and hobby websites where young people interact with others of a similar interest are often perceived as having more personal relevance to the young person as the topic under discussion is of special interest to them. The information being exchanged is often in direct response to questions or queries.

Instant messaging services, such as MSN and Yahoo Messenger, have a very personal role comparative to other social networking services. The immediacy of the exchange of information makes these websites purely about direct interaction and communication rather than entertainment.

Despite other websites such as Facebook, MySpace and Bebo offering an instant messaging function, young people did not claim to use these websites for this function. At the time, the young people involved in the research were much more likely to use MSN and/or Yahoo Messenger for instant messaging.

As overviewed above, and in Section 5.2, as children age the different social networking websites tend to take on different roles. Invariably, use of these websites is initially for games and entertainment. The user then moves to being a passive receiver of content (usually for entertainment) and later an active creator of content.

6.4 How children and young people perceive online vs. real world interactions

The perceptions of the different roles of particular websites provide some indication as to how interactions online can be perceived very differently to interactions offline. For example, for most children their entry into social networking services begins through games and entertainment, often through a multi-player game website such as Club Penguin. Club Penguin encourages children to choose the appearance of their ‘penguin’ and to create the environment in which they live (the igloo they have as their home). While children may understand that they are interacting with other children through their penguins, they still largely perceive the experience as a game.

The idea of social networking interactions being part of a game is continued to some extent as children grow older. For example, the online profiles that young people create for themselves are similar to creating a character. The interactions they experience are often with multiple users simultaneously, much like with multiple characters in a game, rather than the more one-on-one or smaller group experience of the ‘real’ world.

The concept that children saw social networking websites as a ‘fantasy land’, ‘a game’ or ‘not being real’ was discussed by a number of parents. Many parents felt that while the interaction was on a computer, children and young people were able to pretend that their interactions did not have real world consequences. This theme is discussed in more detail in Section 7.5.
07
Perceptions of risk and cybersafety
7.1 Overview

Perceptions of risk and cybersafety can be divided into (1) general online risks and (2) risks that are considered specific to the use of social networking services. The main risks associated with online use in general were the potential for viruses to be downloaded and for accidental exposure to graphic or explicit materials, while risks associated with the use of social networking services included the potential for predatory behaviour by other users, risks associated with webcam use and exposure to cyberbullying.

7.2 Online risks

Children and parents who participated in the qualitative research all perceived the greatest risk of online activity to be that of contracting computer viruses from downloaded information, pictures and videos. All children and young people, regardless of age and gender, were conscious of this risk, it being the main online risk communicated to them by their parents.

“You do not open pop-ups because they might have viruses.”
(eight-year-old girl)

Experience of computer viruses was also commonplace among a majority of children and young people. Many had experienced viruses, or perceived them as a possible risk, when undertaking online activities including:

> interacting on social networking services;
> simply looking at profiles;
> general website use; and
> conducting research for homework or for other interests.

After computer viruses, parents were particularly concerned about their children’s exposure to graphic material, especially accidental exposure to pornography and violent material that may be accessed via ‘pop-ups’ from otherwise benign websites. Few parents felt that their children would actively look for this type of material.

“If it wasn’t on the internet, they wouldn’t really come across it. It is just too easy now for them to be exposed to things that they are not old enough for.” (Parent of eight to nine-year-old girl, also with a teenage boy and girl)

7.3 Social networking risks: Deceptive contact

Children and parents perceived the main risk of social networking services as being the potential for stalking or other predatory behaviour. This concern had clearly been communicated to children and young people, as all identified the main risk of using such websites to be that people could pretend to be someone they were not.
However, perception of this risk varied across different age groups. Children and young teenagers were more likely to perceive that the threat of a predator or a stalker from use of social networking services could become a reality. That is, they were more likely to believe that a predator was an actual physical risk:

“… [be]cause someone could find out where you live and come and get you.”
(eight-year-old girl)

“They could be an old man who is pretending to be 16 so they can chat you up … cause he’s some paedophile.” (14-year-old boy)

“People lying to you saying they could be a dirty old man. These risks mostly happen in chat rooms like MSN.” (13 to 15-year-old girl)

Older teenagers were less likely to perceive that the potential threat of a predator could manifest itself in reality. While they accepted that there was high risk of interacting online with someone who lied about their age or gender, older teenagers did not tend to perceive that predators could become an actual physical risk when using social networking services, as none had actual experience of a predatory or stalking situation.

Instead, the key concern for older teenagers was being deceived about another person’s identity online. Older teenagers were clearly very conscious of the possibility of people lying about their age and gender online. Both genders in this age group found the potential for the unknown person they were interacting with to be someone much older than themselves unappealing and believed they were more likely to experience this danger than a physical stalker or predator.

“If someone random has added you, you are never going to be completely sure that you are actually talking to who they say they are. Especially if you are looking at him and think ‘oh he’s alright, he’s my age, I’ll write something back’—you never actually know.” (16-year-old girl)

“… scary knowing that you could be thinking that it is someone your age and it is actually an old person who has nothing better to do with their life but chat up young people.” (15-year-old girl)

“Some paedophile talked to me on Bebo, she’s like 25, I went on her account and there were all these people saying like you’re a weirdo, go away, and she’s like … I went on my cousin’s account and said to talk to me for a bit because I’ve just moved here and I went on there and there’s all these guys saying don’t talk to me, who are you. It was pretty weird.” (15 to 17-year-old boy)

7.4 Social networking risks: Webcams

Girls also strongly identified risks associated with webcams. While it was acknowledged that webcams are a useful tool to talk to friends and family they knew personally, most older teenage girls had some experience of the possible risks associated with its use. The main risks associated with webcams identified by older teenage girls included the person on the other end acting in a lewd or indecent manner, or material they had sent to one contact being disseminated to others. Most older teenage girls had either experienced one of these scenarios or knew of someone who had:

“My cousin I was sitting next to her and she’d just accepted it. My grandma just came from Turkey and she’s really religious, and this guy started stripping, and as my grandma walked past it happened …” (16 to 17-year-old girl)
However, using a webcam was also identified as a means of sorting through which invites from strangers (‘randoms’) may be more legitimate than others. Older girls identified that they regularly received invitations from strangers with requests for webcam use. While not articulated, it was inferred by respondents that these reasons were usually sexually motivated.

“Some guys want webcam, and want you to do other things on the webcam, which is pretty stupid…”

Therefore, it was the strangers that did not request webcam communication that were looked on more favourably, and that girls were more likely to respond to. The experience of one older teenage girl highlights this perception:

“This fellow didn’t ask for webcam. I felt secure that he wasn’t some naughty guy … I just talked to him for a while, and it was coming to holidays, and it was ‘why do not we meet’. He lives in Cronulla. So we ended up going out for a while, but that was that. He is a great person and I’m happy I met him; I got to meet more people from that. It was out of my zone. I’m from the North Shore, and it is good to meet people from another area of Sydney.”

7.5 Social networking risks: Cyberbullying

Awareness of cyberbullying as a potential risk

Neither children nor parents perceived cyberbullying to be a risk of social networking website use until teenage years. This is because cyberbullying is mainly perceived to be associated with the social networking services such as Bebo, and MySpace, and it is only from the ages of 12 to 13 that most of the focus group attendees began to use these services.5

However, when prompted, children under 12 did identify swearing and minor name calling as behaviour that could be considered a form of cyberbullying. Younger children knew it was something they should not do, and claimed to follow the rules that were outlined by website providers relating to these issues. For example, users of Club Penguin were very aware that they could be stopped from using the service if they did not follow the rules against swearing or calling others names.

All teenagers (13 to 17 years) were aware of the potential risk of cyberbullying. Most girls saw it as a real and relevant issue, whereas boys claimed to have little exposure to anything they would perceive as bullying.

Older teenage girls identified that the use of social networking websites to bully was an unfortunate extension of what was happening in the school yard among teenage girls. For girls, arguments and disagreements with others is commonplace in the teenage years. Social networking services play a significant role in how teenage girls communicate with each other, and as such become another medium for this behaviour.

In contrast, boys use social networking services mainly for pursuing interests (including the interest of girls) and entertainment. While part of the entertainment value of these websites may be playing practical jokes on friends and others they know, this behaviour tends not to be perceived as bullying, but as a normal part of the way male friends interact with each other. Both parents and boys in the group discussions accordingly perceived cyberbullying as less of an issue for boys than for girls. It was claimed that arguments and disagreements between boys did not tend to happen online, and if they did, they were not seen as serious and typically reconciled by simply ignoring each other for a time.

---

5 As the key focus of the research was the internet, including social networking websites, the research did not explore the extent to which bullying was experienced via text messages to mobile phones. Moreover, ‘cyberbullying’ was not given a precise definition at this stage of the research project. Questions were aimed at identifying a level of awareness of the issue, rather than trying to gauge a level of prevalence.
“... you just block them—if it gets out of hand you just go block ...”

“Yes, you just block them and they can’t see you and don’t know if you’re online or not ...”

Defining cyberbullying
While ‘cyberbullying’ was not given a precise definition at this stage of the research project, and questions were aimed at identifying a level of awareness of the issue, some general definitions did emerge.

Broadly, girls define cyberbullying as saying hurtful things to others. There is a change in perspective of what is hurtful as girls get older and use social networking services with greater frequency. Younger teenage girls, those in grade 8 and 9, were more likely to find name calling and swearing as hurtful. Older teenage girls, those in grades 10 and 11, were more likely to see this behaviour as part of normal interaction between girls in both online and offline environments.

“If it is just like ‘you are a slut’ or something like that, then I do not think many people would care ...” (15 to 17-year-old girl)

Older teenage girls were more likely to identify personal attacks as bullying behaviour. These were defined as comments specifically about an individual or their family and friends, and included comments on:

- appearance;
- past experiences;
- family and friends;
- information told to another in confidence; and
- exaggeration of incidents.

The quotes below illustrate some examples of what older teenage girls identify as bullying:

“It is more like picking on things that are personal, like maybe ... on your face or things like that, I’d get upset about—but if it was like ‘you are a slut’—I’d just be ‘whatever’ ...”

“Or something that happened on the weekend, that you do not want anyone to know, and she brings it up in comments ... or something about your appearance as well ...”

“Or something you’ve done and people bring it up, things from the past, that you want to forget ...”

“I think if they are saying something and then say ‘this person said something about you’ and that person is your friend, then you do not want to believe them ...”

“Also if they haven’t got the facts right, like if it is a little bit about something and they go and blow it up fully into something that it never was, that really bugs me ...”
Actual effect of cyberbullying

Both the content and speed of information exchange make cyberbullying an issue for girls, with the public nature of the arguments, as well as the actual words said, causing the greatest concern and offence. The faceless nature of the online environment was seen to encourage the inclusion of more hurtful and extreme content in comments compared to what might be said face-to-face. In addition, social networking websites allowed the comments to be easily distributed to multiple people, thus increasing their impact.

“… people say things to you that they wouldn’t say face-to-face … it’s easier”
(15 to 17-year-old girl)

“You can spread rumours easily … it just goes out to people.” (15 to 17-year-old girl)

“In comments, if you are writing this sort of stuff in a comment for everyone else to see, then it is not right.” (15 to 17-year-old girl)

Parents agreed that cyberbullying was more of an issue for girls than boys. Like older teenage girls, parents were likely to see that the ‘normal’ arguments of teenage girls were able to be intensified by the faceless medium of the internet. Some parents attributed the greater intensity of the arguments on the internet to the interactions being perceived part of a game, rather than actions with real-life consequences:

“It just makes it all worse; they just say things they wouldn’t say to each other in person.” (Parent of 13 to 17-year-old girl and boy)

“I’ve got her password and I check to see what her and her friends are writing to each other. I tell her to not say anything that she wouldn’t say to their face.”
(Parent of 13 to 17-year-old girl)

“They do not see it as real … it is a fantasy land … it is not real to them.”
(Parent of 13 to 17-year-old girl)

Parents perceived that bullying would have the greatest impact on less confident girls. One of the key issues raised after watching the Laura’s Ordeal video clip from ACMA’s Wise Up to IT DVD was that not all girls would tell someone about the situation, especially those who may not be as socially outgoing or who are less confident and familiar with what is said and done on social networking websites. The potential for bullied girls to harm themselves particularly concerned parents.

“At least she told someone about it.” (Parent of 13 to 17-year-old)

“… dealing with it by herself … it is like those girls that committed suicide.”
(Parent of 13 to 17-year-old)

It is this perception of a divide between ‘reality’ and online interactions that seems to contribute to teenage boys not identifying cyberbullying as an issue for themselves.6 Teenage boys see the internet more as a form of entertainment and a means to pursue interests, and thus are more likely to see what is said on social networking websites as part of its entertainment value rather than as direct personal attacks. Boys were also more likely to claim that they would simply avoid the situation if they did not like what was being said:

“It is so easy to ignore, it doesn’t really matter …”

“I do not see why they’re so worried about it, nothing’s going to happen, it is just over the internet …”

“Yes, some kids from our school had it done to them, they made a big thing about it … They all complained but it is like nothing …”

---

5 Please note: the potential for the sample to have consisted of quite confident teenage boys should be taken into consideration.
“Yeah, just stop it, just leave the conversation; you can just ignore it so easily …”

“No big issue. It is an issue but I’d be more worried if someone came up and said it to me …”

The real risk of negative online interactions identified by boys was the potential for arguments or disagreements to manifest as physical confrontation. An example referred to was of an incident that occurred approximately at the time of the fieldwork where a teenage boy was stabbed outside of his school as a result of a ‘rap’ song posted on a social networking website. Another example is shown in the quote below:

“My friend on MySpace … some guy was saying he was going to smash him, then it was like an organised fight and the cops found out. He was just sending all these emails on MySpace saying he was going to smash him. He would have got smashed. He didn’t have anything to do with it. He called their school pussies or something and then this guy started sending all these emails and stuff and getting all his friends …”

7.6 Online risks and offline risks

Many children and parents involved in the research perceived that the physical risks posed by everyday life exceeded any potential for online danger from social networking website use. For example, face-to-face bullying was perceived as a greater risk to a child’s mental state than cyberbullying. And for parents, the potential of being abducted by a stranger met face-to-face was seen as a far greater risk than any online risks:

“I let my daughter go running at night and there is probably much more chance of her being abducted that way than online.” (Parent of 13 to 17-year-old)

“I think I read that there were 1,000 paedophiles in Australia out of 13 million or 20 million people. This is a fairly low ratio.” (Parent of 10 to 11-year-old girl)

For children and young people, the key difference between online and offline risks is the potential deceptive behaviour that manifests from not being able to interact with someone in person.

Older teenage boys from one of the research discussion groups also highlighted the overlap that is possible between online and offline interactions. These particular boys had experienced the online organisation of a physical fight that was to take place offline.

Parents’ perceptions about the relative risks of online and offline behaviour was partly attributed to the common belief that prevention of bad online behaviour could be achieved by limiting exposure. Many parents felt that it was a matter of simply blocking bullies or strangers, reporting them or turning the computer off.

“Surely you just block or report someone if they are being abusive.”
(Parent of nine to 10-year-old girl)

“If someone is hassling you surely you simply switch the computer off.”
(Parent of 13 to 17-year-old)

While this kind of action may be an effective means of preventing cyberbullying and unwanted attention from strangers for many teenagers, it is likely that some may not consider these options as a real solution. The ways in which different teenagers may react to these issues is discussed in further detail in the following sections.
Segmenting teenagers
8.1 Overview of the segments

Five different groups of teenagers were identified from the qualitative research, differentiated on the basis of their claimed behaviour and attitude towards risks associated with social networking services. Each segment has been identified with a name, which has been developed by the researchers as part of this project, and is intended as a descriptive label of the behaviour and attitudes exhibited or claimed by individuals in each group. Please note that these segments have not been quantified and should be currently considered as hypothesis.

The following descriptive labels have been developed to identify segments of teenagers emerging from the qualitative research:

> Active Risk-takers;
> Responsible Risk-takers;
> Vulnerably Influenced;
> Specialist Seekers; and
> Claimed Conformists.

These segments are meant to identify groups of teenagers according to the following characteristics:

> personality type displayed by individuals in a group setting;
> claimed online behaviour;
> the role or purpose that social networking services seemed to have for them; and
> knowledge and attitudes towards online risks.

While there are overlaps between segments, key differences still exist. For example, while Active Risk-takers and the Vulnerably Influenced claimed the same online behaviour, they were different in all of the other characteristics considered. Alternatively, although Active Risk-takers and Responsible Risk-takers shared many characteristics, they were distinct regarding their online behaviour.

Table 3 below provides a summary of the variables used and how they applied to the different segments. A full description of each of the segments is provided in the next section.
<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>ACTIVE RISK-TAKERS</th>
<th>RESPONSIBLE RISK-TAKERS</th>
<th>VULNERABLY INFLUENCED</th>
<th>SPECIALIST SEEKERS</th>
<th>CLAIMED CONFORMISTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personality displayed in group situation</td>
<td>Outgoing &amp; confident</td>
<td>Quieter</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Knowledge and attitudes to risks</td>
<td>High level of knowledge</td>
<td>Demonstrated knowledge of mitigating risks</td>
<td>Likely to seek assistance when a problem occurs</td>
<td>Demonstrated knowledge of mitigating risks</td>
<td>Demonstrated knowledge of mitigating risks</td>
</tr>
<tr>
<td>Role of social networking services for the teenager</td>
<td>To expand social networks</td>
<td>To maintain social currency</td>
<td>To maintain social currency</td>
<td>To pursue interests or hobbies</td>
<td>To pursue interests or hobbies</td>
</tr>
<tr>
<td>Claimed online behaviour</td>
<td>Only uses webcam to interact with known friends</td>
<td>Have used webcam to interact with strangers</td>
<td>Have used webcam to interact with strangers</td>
<td>Have uploaded personal information onto website</td>
<td>Have uploaded personal information onto website</td>
</tr>
<tr>
<td></td>
<td>Have met someone face to face after meeting online</td>
<td>Have accepted invitations from strangers or sent invitations to be friends with strangers</td>
<td>Have accepted invitations from strangers or sent invitations to be friends with strangers</td>
<td>Have used webcam to interact with strangers</td>
<td>Have used webcam to interact with strangers</td>
</tr>
<tr>
<td></td>
<td>Have interacted online with strangers</td>
<td>Have interacted online with strangers</td>
<td>Have interacted online with strangers</td>
<td>Have used webcam to interact with strangers</td>
<td>Have used webcam to interact with strangers</td>
</tr>
<tr>
<td></td>
<td>Use multiple social networking services</td>
<td>Maintain public profile pages</td>
<td>Maintain public profile pages</td>
<td>Use multiple social networking services</td>
<td>Use multiple social networking services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
8.2 Describing the segments

Active Risk-takers

The teenagers identified as Active Risk-takers were very outgoing and confident in group discussions. These teenagers claimed to have engaged in a number of high risk behaviours, including:

- having met someone face-to-face after meeting them online; and
- using webcams to interact with strangers and/or in another risky manner.

These teenagers claimed to be very familiar and confident in their use of social networking services, which were an important part of their social behaviour and were actively used to expand their social networks. These teenagers commonly made use of multiple social networking services, and tended to have ‘public’ pages which were accessible by ‘non-friends’ (strangers).

The Active Risk-takers segment was highly knowledgeable about the more obvious online risks, and held the attitude that the risks were all part of the experience. Given this knowledge, they would take active steps to mitigate potential risks from their online behaviour, such as:

- ensuring that when first meeting someone in person they did so in a public place;
- ‘Googling’ someone’s name before meeting them in person;
- chatting on MSN Messenger with someone they met online before meeting in person. (Being one-on-one and in real time, instant messaging is seen as an intimate platform to be more open and honest, which provides an overall reassurance); and
- for boys, talking to a girl online for a while before meeting with her in person to ensure that she was a real person and that a practical joke was not being played.

Possibly because they have a strong online presence, Active Risk-takers are susceptible to cyberbullying, with some claiming they had experienced online bullying from strangers as well as offline friends.

Teenagers in this segment believed that it was their own responsibility to ensure their own safety regarding online and resulting offline activities. As this segment believes they have extensive knowledge of the more obvious online risks and how to avoid them, they may be resistant to information on risks they may not be aware of, unless it comes from a credible source, such as peers.

Responsible Risk-takers

Responsible Risk-takers were similar in many ways to Active Risk-takers, and had similar levels of confidence in talking about their experiences in group discussions. However, while Responsible Risk-takers claimed to engage in some risky behaviour, they tended to not go beyond certain levels of risk; that is, they would draw a line with regard to their behaviour. The risky behaviour that characterised Responsible Risk-takers included:

- having ‘friends’ they did not know personally; and
- accepting invitations to be a friend from ‘hot randoms’ (people they met online who they considered attractive).

Participating in social networking services was an important part of the social behaviour of Responsible Risk-takers and was actively used to expand their social networks. These teenagers were likely to make use of multiple social networking services, although they often had a favourite. Some claimed to have public pages, while others said they actively used the websites to view the public pages of others so as to know them better.
While Responsible Risk-takers have similar levels of understanding of online risks as Active Risk-takers, they are unlikely to engage in subsequent high risk offline behaviour. For example, they:

> may talk to a stranger online, but would be unlikely to agree to meet in person;

> may use webcams with a stranger only after asking them to turn on theirs first to make sure they are the person they claim to be; and

> will upload some personal details and photos, but take care on how specific the detail is.

In common with the Active Risk-takers, Responsible Risk-takers are susceptible to cyberbullying, due to their level of risk taking.

Teenagers in this segment perceive it is primarily their responsibility to mitigate the risks of their online behaviour, but would be more likely than ‘Active Risk-takers’ to seek assistance from parents, police or friends should a problem eventuate. Girls in this segment, for example, are likely to tell someone if a problem occurred online.

Vulnerably Influenced

The Vulnerably Influenced segment appeared to be less active in their use of social networking services. Teenagers on whom this segment is based appeared quieter in group discussions.

Social networking websites appeared to be more important to these teenagers for helping to maintain their social currency than for actively expanding their social networks. These teenagers were more likely to claim that they used the websites because everyone else did (to ‘fit in’) and to be able to have something to talk about at school.

This segment was less likely to claim to have engaged in high risk behaviour, but their responses during the group discussions indicated they had potential to do so. Many claimed they would meet someone they had met online in person if given the opportunity. This group also tended to be more likely to claim to have a ‘public’ page accessible by strangers. Based mainly on interpretation of their responses in the group discussions, these claims to high risk behaviour appeared to be based on the belief that ‘everyone’ does it.

The key concern for this segment is whether they are fully aware of the risks of online activity. As they tend to have less exposure to social networking services than more active users, teenagers within this segment may be less able to fully comprehend potential risks associated with their behaviour. They were also less likely to volunteer information on how to avoid or mitigate risks, suggesting that perhaps they were unsure on how to do so.

Lack of awareness and experience of risk could result in this segment not understanding what action they could take should they be put in an unwanted situation, and being less likely to seek help from parents or police when necessary.

Specialist Seekers

Specialist Seekers generally claimed to follow the rules on social networking services. This segment includes teenagers who use social networking services primarily to discuss their interests, lifestyle choices or hobbies. With their focus on specialist interests, this group tends not to use social networking services as a means of expanding their general social networks. These teenagers were more likely to claim to have private pages on websites and/or to be members of a special interest forum.

Sport was a commonly identified type of specialist interest. Music and lifestyle interests, including emo or goth subcultures, were also identified as special interest, (although none of the focus group participants claimed to visit emo or goth websites as they appeared to have a negative connotation).
This segment actively seeks out and interacts online with others who have similar interests. Given they are under the assumption that all others in the online community are there for the same purpose of the shared interest, these teenagers are likely to trust those they meet online in this type of forum. In contrast, they would be highly unlikely to have the same level of online, and potentially in person, interaction with someone they met on a website they perceive as more for social purposes, such as the social networking websites of Bebo and MySpace.

Specialist Seekers would be likely to mitigate risks despite not necessarily recognising there are risks. For example, these teenagers would be highly likely to tell their parents if they had arranged to meet someone in person after first meeting online. Risks for this segment may arise if they, or their parents, did not perceive that the same contact and privacy risks existed when using special interest websites and forums as they identified with the general social networking websites.

A subgroup of the Specialist Seekers segment use social networking services to seek out negative or harmful material, such as anorexia websites. This segment did not self identify. Instead, parents or other teenagers identified that they had children or friends (respectively) who sought out this type of contact.

Parents and friends who identified this subgroup tended to perceive that, since exposure to these websites was due to active searching by the child or teenager, there was little to be done to limit their access to these services.

**Claimed Conformists**

This segment was developed to account for the discrepancies identified between the behaviour and attitudes claimed by many of the respondents on the bulletin board and those stated in the group discussions. Analysis revealed that the responses on the bulletin board were not as indicative of risky behaviour as the group discussions. The differences in responses between the two forums could be due to either:

- participants exaggerating behaviour when in the presence of their peers during group discussions; or

- participants less likely to admit to risky behaviour on the bulletin board.

Based on the group discussions and triads, the majority of children aged eight to 12 had the attitudinal and behavioural attributes of the Claimed Conformists segment, but few, if any teenagers claimed these behavioural attributes. However, as it is likely that teenagers such as this do exist in the broader community, this group has been included in the qualitative segmentation of teenagers.

The key characteristic of this segment is that they will claim that they do not engage in risky behaviour on social networking services. Taking into account the factors outlined above, there are likely to be some teenagers who do not undertake any risky behaviour. However, it is also possible that some who do fall into this segment engage in some low risk behaviour without identifying it as such.

Teenagers in this segment know the risks of social networking services, and claim to follow all the rules to avoid risks. These teenagers would claim:

- only to have private pages on social networking services;

- only to have ‘friends’ whom they know personally;

- never to upload any personal information about themselves, with the exception of pictures of themselves (ensuring that it is not in front of an identifying location) or to talk about hobbies or sports.
09
Content, contact, and privacy risk behaviour
9.1 Content

Viewing internet content was acknowledged to include a number of risks, including potential exposure to violent content and pornographic/sexual material. Children noted they were easily able to view this type of content on the internet via pop-ups, downloads, file sharing (for example, LimeWire) or unfiltered image searches. The risk of being exposed to such content led to a number of concerns amongst children and young people, including computer viruses, getting in trouble with their parents, and exposure to explicit material.

Exposure to violent or sexually explicit material on the internet occurs at all ages among eight to 17-year-old girls and boys, with the exposure ranging from accidental to sought after.

At a young age, it is more likely that discovery of such content is accidental than intentional. For most, it was something that just happened when using the internet. While they might identify it as ‘gross’, some did admit that they would often try to work out what the material was if they came upon it accidentally. Mistyping words when searching on the internet was common, for example, a seven-year-old had entered ‘Dora the Sexplorer’ (instead of Dora the Explorer) and a 12-year-old had mistyped ‘Hotbod’ (instead of HotBot the search engine). In addition, pop-ups did not always contain the content that was expected.

“I was on Hello Kitty looking for a present for my cousin who likes that stuff and there was a pop-up, and I clicked it … and it wasn’t the Hello Kitty.” (nine-year-old girl)

“I clicked on a pop-up and it was a picture of man and woman and he was … you know, and she was lying back with her eyes closed … she looked like she was asleep.” (eight-year-old girl)

In particular, boys indulged their curiosity by actively seeking graphic material. This did not only include sexually explicit material, but stunts and daring acts. Often material was sought out of personal curiosity, for example, one 10-year-old boy typed ‘breasts’ into Google, while others talked about violent online games:

“At school, games [gaming] is a common discussion so if someone mentions something I will Google it when I get home. One of the games was called ‘kill the Tellytubby’.” (11 to 12-year-old boy)

Both older girls and boys seek material to share with friends, as social currency at school or for a joke. In some instances, it was evident that the more shocking and dangerous the material the better, particularly if it was of a sexually explicit or violent nature:

“A few of my friends go looking for really dirty porn but it’s all a joke.”

(16 to 17-year-old girl)

“I’ve seen people commit suicide on YouTube—my friend sent me a link—I found that a bit scary. I saw some guy jumping off a building…” (16 to 17-year-old boy)

While violence held appeal for many boys, it was a concern for girls. In particular, eight to 12-year-old girls were especially concerned about discovering violent images, claiming these were not pictures they would want to look at and that they would be worried about their parent’s reaction.

“I am not allowed to go on bad sites that might have images of guns or blood.”

(10-year-old girl)
For boys aged 10 years and over, violence was often an integral part of the games they played online. Boys aged 16 to 17 years suggested that sharing links to violent content was regularly used as a ‘shock tactic’ to fuel communication with friends. For these teenage boys, part of communicating with male friends online included sending links to content such as YouTube videos, which containing violent or graphic material. For some, the more violent or shocking the material, the better.

Whether accidental or sought after, what was done with ‘risky’ material depends on the type of person. While some teenagers claimed they would seek out the material and forward links to their friends, others would only forward links when received from others. Still other teenagers might view links to risky material, but would probably close a webpage if it was not of direct interest to them. The most cautious could not click on links or pop-ups, and would close a webpage and tell a parent if they accidentally opened it.

Young people were most concerned about the consequences for their internet use that they associated with accessing risky material. The first of these involved their parents finding out, leading to a telling off and a potential ban from using the internet. The second was exposure to viruses, which again would lead to a telling off from parents, but in addition could mean they would be unable to use the computer and that their future internet access would be restricted or monitored more strictly.

9.2 Contact

While predator risks are forefront in children and young people’s minds, other risks potentially arising from online content are not an active concern. Those of primary school age (eight to 12 years) did not actively seek or desire contact with people they do not know and mostly interact with their close-knit circle of friends at school. For them, the danger of contact is not as ‘real’ or likely to happen while under close supervision from parents. Those of high school age (13 to 17 years) are forming friendships, and their learning and curiosity expands both offline and online. The fun and freedom associated with growing up and experimenting outweighs any potential risks and there is a mentality of ‘it won’t happen to me.’

Parents and young people recognise that social networking services are open to people all over the world. A few parents see beyond the ‘stranger danger’ and believe social networking websites are an added dimension to their children learning about different countries and cultures through the people they meet. In reality, many young people are aware of the global nature of the environment in which they are participating, but are more interested in finding people who live in the same town as they do. The exception is those who share a common interest.

“I like to play chess and on MSN you can accept invites from people all over the world to a game of chess, so I do.” (12-year-old boy).

A proportion of teenagers were happy to accept ‘friend’ invites from strangers of the opposite gender, particularly if they were seen to be good-looking and of the same age. This was more common among those in grades 10 and 11 (15 to 17 years).

“You look at their age. If their age is alright … where they live … if they’re hot …” (15 to 17-year-old girl)

“Yeah, it’s all girls. I have boy contacts but I just do not talk to them. If they talk to me I don’t talk back, I just ignore them …” (13 to 15-year-old boy)

“You don’t generally want to make friends with older people because you’re not ever going to meet up with them or anything …” (15 to 17-year-old boy)
Most claim that accepting ‘friend’ invitations went no further than ‘friends of friends’, but it is unclear what this actually means in reality. It could mean ‘online friends’ of ‘online friends’ or ‘online friends’ of ‘personal friends’.

“I think Bebo is better in that way because they have the ‘friends in common’ thing, but if you see someone has added you that you do not really know, and they’ve got all these friends that you know, you can say ‘she’s alright’ …”

“I basically just look at the ‘friends in common’, if I know people who know the person that I do not know, then I’m more likely to add them …”

“Or you look at the comments your friends have sent them …”

But many teenagers did not limit their interactions to only those they knew personally, even when restricting their profile to ‘private’. Websites such as Bebo and MySpace were perceived as having a key purpose of getting to know other people better, and that meant people beyond those they knew in person. The group discussions indicated this was a common behaviour.

“It is mainly friends of friends, random people that you talk to and never end up seeing them—until they ask you to …”

“Well obviously you do not physically know them; you just know them through what they’ve told you. Unless you’ve seen a webcam you can’t tell what they look like or their actual personality and stuff like that …”

“I have quite a few fans on YouTube as a result of my model rollercoaster video … I sort of like the attention I get off YouTube.” (16-year-old boy)

Contact is one of the key attributes that differentiates the segments. Active Risk-takers will meet in person with someone first met online, use webcam and accept strangers’ requests with little vetting. Responsible Risk-takers are unlikely to meet offline with someone they have first met online, but will invite strangers as friends and may use webcam after seeing the other person first. The Vulnerably Influenced possibly would meet in person with someone if asked and would invite strangers as friends and chat to them. Specialist Seekers are likely to seek out others and accept invites from others with similar special interests. Claimed Conformists are likely to only have friends online that are friends offline.

Cyberbullying was most likely to occur amongst teenagers. Children aged eight to 12 years may have experienced ‘name calling’ or ‘silly remarks’ but nothing that would be considered bullying or be taken seriously. Cyberbullying becomes more prevalent at high school. For example, one 13-year-old girl mentioned a fake Bebo profile made in someone’s name with photos of that person and derogatory remarks. Another girl commented on the risk of adding friends of friends who might then gang up and turn against the person who added them.

The risk of being publicly bullied and made to ‘stand out’ online, with the danger that what happened online could continue at school is a very real one for teenagers. There is also concern that they could be the subject of a practical joke, and it was acknowledged that there is potential for jokes to escalate out of control, with someone always ‘having to go one better’.
9.3 Privacy

Often young people choose to be open and expressive. The option of protecting their privacy online often falls by the way-side in favour of wanting their profile page to attract attention. This can be done by using lots of detail (for example, the use of photos and skins), welcoming attention from the opposite sex (particularly teenagers) and welcoming friend requests from those with similar interests. An environment scan in this area indicated that risky or suggestive outward expression is commonplace in some young people’s public profile pages.

The willingness to make personal information public differs widely across the segments. Active Risk-takers have a ‘public’ detailed profile page and are happy to upload and give out personal details. Responsible Risk-takers are more likely to have a private profile page and give consideration to the personal details they give out. The Vulnerably Influenced could be influenced to have a public page and are likely to give out personal details if asked. Specialist Seekers are most likely to have private profiles and are more open to giving out information about themselves to people/forums with a similar interest. Claimed Conformists have a private profile page with few personal details and will not give out their personal details.

While privacy is not always front of mind for young people, they do express some concerns. Children and young people worry that if someone else discovers their password or accesses their personal account they could delete or alter information, send abusive messages from their account or make them the victim of a practical joke. In addition, they are aware that accidentally divulging personal information could lead to negative consequences, for example information such as letting people know that their family is going away on holiday could be misused by an acquaintance.

Despite these concerns many claimed they would give someone, usually their best friend, their password in certain circumstances. This may be, for example, if they struggled to remember it, they were not allowed online and they wanted their friend to upload photos from the weekend, or they were no longer using their account and thought someone else might as well make use of it. In addition, they might give their real name if everyone else seemed to be using their full name.

“I have my full name on Facebook. I didn’t want to do it but I realised that everyone else and all my friends had.”

9.4 Reasons for engaging in and impact of online high risk behaviour

Children and young people did not tend to identify their behaviour in terms of risk, or to ascribe a degree to it. Those who engaged in high risk behaviour primarily did so because others did, and therefore their behaviour was generally reflective of those around them. However, other motivations for high risk behaviour exist, including fun/excitement, curiosity and boredom.

Engaging in high risk behaviour can have varying levels of impact as shown in Figure 3. Some behaviours have consequences which would deter future repetition. In others, the consequences may not be so severe, and therefore these behaviours may be repeated.
Explicit material continues to be sought out, regardless of its severity and how hard hitting or explicit it may be.

“I’ve seen someone committing suicide on YouTube.” (16 to 17-year-old boy)

While the content may be considered ‘gross’ or disturbing, this is unlikely to discourage children or young people from looking at other explicit material in the future, as such content contains to carry a social currency amongst friends.

Webcams can be a temptation for teenagers to take communications with the opposite sex to the next level. For some people, webcam use may be employed as a preliminary precautionary measure before actually meeting with someone in person. However, girls are particularly wary of webcam usage, and for older girls, behaviour that has initially been seen as harmless fun has resulted in unwanted outcomes, including indecent exposure and an abuse of trust.

“My friend was on a webcam and this guy flashed her.” (16 to 17-year-old girl)

“My friend danced naked with her friend on webcam but then these guys put it all over the internet.” (16 to 17-year-old girl)

Most downloaders had encountered problems that could potentially deter future downloading, including receiving viruses from downloads and pop-ups that damaged their computer, and got them into trouble with their parents.

“There was this MSN link that said ‘is this you in this picture’ and when you clicked on it a virus was downloaded.”

“I only looked at porn once because I got a virus that destroyed my computer. Now I just wouldn’t risk it again.” (13 to 15-year-old boy)

Depending on the level of damage to the computer or telling off from parents, viruses can discourage future accessing of downloads and pop-ups.

Becoming the subject of a practical joke by using other people’s personal information, can be an example of risk taking going too far:

“I created a fake MSN and got a date for my 18-year-old brother on the internet. He was very excited until I told him and he just said he would get me back.” (16-year-old boy)

“If you post photos on Bebo, someone can edit them and put your head on a naked body and print it off and embarrass you.” (13 to 15-year-old girl)

Improper use of other’s personal information could be classed as cyberbullying:

“Some guy at school hacked into this kids account and sent loads of abusive stuff to his friends.” (16-year-old boy)
Older siblings influence risk-taking behaviour by setting the precedent. They can influence their younger counterparts' behaviour in a number of ways, through allowing them to watch what they do from an early age, and thus advancing their younger sibling’s internet capability and social awareness. They often teach them how to use the computer and internet, setting up accounts for younger siblings and setting the level of trust between parent and child. This level of trust often then applies to all younger siblings in the family. For example, if the eldest is seen to demonstrate responsible behaviour online, parents are more likely to be trusting of all their children, however, if they are irresponsible then parents are likely to monitor all of their children more closely.

Peers influence risk-taking behaviour by setting the social standard. Trends set by peers include determining what profiles should include, seeking out the next best violent game, determining which online website/forum is best for interacting, and finding and forwarding the next most explicit/shocking material possible. All children and young people feel that a basic social online currency is necessary.

7 In-home triads revealed siblings as young as three years of age were watching older siblings on the internet.
Management of online risks
The management of risk depends on whether or not the risk is perceived to be present. While many are aware of the potential risks of being online, not all acknowledge their susceptibility to risk. Some have an ‘it will not happen to me’ mentality, some ‘I give as good as I get’. Others believe it is about being careful:

“I haven’t seen any risk using YouTube, MSN or MySpace; although the schools and government tell me that I am in danger being online. As long as you are careful there aren’t really any risks.” (16 to 17-year-old boy)

There are four main ways that young people manage risk, and these include:

> abiding by the rules and advice given by parents;
> using common sense;
> learning from experience; and
> resilience.

Abiding by the rules and applying commonsense are relatively easy strategies, which tend to be used by the eight to 10-year-olds. Methods this age group might use to mitigate risk would be giving only parents their password, scanning downloadable files, and reporting someone who is behaving inappropriately or offensive material they come across online.

However, many children and young people do not want to abide by the rules and apply commonsense. Learning from experience and developing resilience is usually a phenomenon of increasing age and exposure to being online. Often the ways teenagers manage risk are learnt through experience; for example making their profile page private after receiving unwanted comments, not using a webcam with strangers after an incident of indecent exposure, or avoiding downloading suspect files or opening pop-ups after they have had a virus.

Resilience to practical jokes and name calling is more a characteristic of Active Risk-takers and Responsible Risk-takers. Their slightly more mature perspective and level of personal confidence allows them to turn a situation around or brush it off:

“If someone called me a slut I would be ‘whatever’ and I wouldn’t really care.” (15 to 16-year-old girl)

While most claim to follow the ‘basic’ safety advice they have been given, exceptions to these rules are quite common.

They would give out their phone number if they were chatting on MSN to a close friend. Many suggested they would add someone as a friend if they were a “common friend”, they lived nearby, they were ‘hot’ or they had a similar interest.

“I am from North Ryde so if they are then they might know people I know, so I’d add them as a friend.” (15 to 16-year-old girl)

Meeting up with someone they had met online was acceptable if their friends went with them (16-year-old girls and boys) or they had checked them out beforehand in some way (16-year-old girls):

“My mum used to go on dating sites and then check out the person by Googling their name, so I would do the same.” (16-year-old girl)
The majority of teenagers considered it was their responsibility to manage the risk of cyberbullying. Although acknowledged as hurtful, it was seen as a part of using social networking services, particularly by those more familiar and experienced with the services. Some questioned the impact of involving parents and/or police, in terms of whether it would have any real result and whether it would just make the situation worse. As bullying was generally seen to come from someone known personally, the more socially confident teenage girls would tend to confront or counter attack, and it is the less confident teenagers that might not report the bullying and try to deal with it alone.

Privacy controls are important in providing young people with the choice to protect themselves. While most young people understand that internet safety is primarily their responsibility, many believe web providers have a duty to allow website users to be safe, and give the choice not to disclose personal information. Privacy control is necessary to reassure parents of a website’s safety. The privacy controls that were valued included the choice of either a private or public webpage, the choice to hide their age, which some girls did to avoid unwanted attention, and the choice to show either their real name or an alias.
The role of parents
11.1 Parents’ knowledge, attitudes and understanding of risks

Two key barriers to the effective discussion of risks between parents and children were able to be identified. The first of these was parents’ knowledge of online risks. The second was whether parents’ perceived that the risks were relevant to their child or not. While most parents claimed to have discussed the obvious online risks with their children, it was apparent that parents limited discussions of risks to what they perceived as likely to be relevant to their child.

Parents claimed that they began to discuss online risks with children when they first started to use the internet. As the children were usually young (around eight to 10 years old) these discussions were limited to topics such as:

- avoiding viruses by not clicking on pop-ups; and
- clicking out of content that might not be suitable as soon as it appeared.

As children got older and began to use game websites with multi-players, for example Club Penguin, Runescape and World of Warcraft, parents would discuss the risk of providing personal details to others. This risk was also discussed with teenagers when they began to use other social networking services, such as MSN. In addition, parents would ensure that they discussed with their child the importance of only having friends they knew personally in order to avoid potential contact risks.

While a small minority of parents claimed to have initiated discussion with their children when they began to use MySpace or Bebo, the majority had only initiated discussions when prompted by an external source such as media reports or school activities. School activities included letters being sent home from school due to an incident occurring in the broader school population, or a workshop or lecture on the topic being delivered to all students.

Attitudes to contact risks

The majority of parents considered that their children would be safe from potential contact risks as they believed that their children only had friends that they knew personally. Many parents were unaware that their children’s profile pages could be made private or public. Those that were aware of this function assumed that their child’s profile page would be set to private. The general perception was that this would make it near impossible for a stranger to interact with their child or to piece together disparate pieces of general information about their child and approach them physically. Parents also perceived that their child would follow the ‘rules’ of not giving specific details about themselves and would therefore be safe from any predator that may ‘hack’ into profiles.

It is highly possible that some parents are not aware of the extent of their child’s online network of friends. The figure below illustrates the differences between those who parents commonly perceive as their child’s online ‘friends’, and who the teenagers in the group discussion claimed they include as ‘friends’. Parents tend to believe their teenage children only have online friends they know in person (off-line), such as friends from school. In contrast, many of the teenagers in the group discussions claimed that they had ‘friends’ who they did not know from an in person meeting.
Attitudes to privacy risks
The potential for their child to upload identifying or personal information about themselves or their families was one of the key concerns that parents held towards their child’s use of social networking services. Due to this, most parents claimed to have had a discussion with their children about the risks of releasing this type of information into a public forum. The key risks identified to children about uploading this type of information was the potential for a stalker or predator to use the information to find the child in real life. Because they had spoken about this with their child, most parents perceived that their child was unlikely to upload identifying or personal material during their use of social networking services.

Most were aware of incidences where another child had uploaded material that could be considered potentially embarrassing. These incidences included:

> using webcams inappropriately;
> posting revealing pictures;
> having conversations with dubious or explicit content.

However, the majority of parents believe that it would not be their own child who would be involved in these type of incidences. Therefore, in contrast to uploading personal or identifying details, parents tended to only have a cursory conversation about the possibility that potentially embarrassing material could be further disseminated to unknown others, if they discussed the matter at all.

Very few parents had even considered the risk of their child’s ‘digital footprint’ until it was prompted in group discussions or interviews. Even then only a few considered it to be an issue that they should be concerned about or should discuss with their child.

Attitudes to content risks
While many parents were unwilling to believe their child would take contact and privacy risks when using social networking services, they were accepting of the risk of inappropriate content being seen or sourced online. Many parents recognised that their children may have a natural curiosity about some material and may view material proffered to them to satisfy this curiosity, even if they are aware that it may be inappropriate. Only a small minority felt that their child would actively seek out inappropriate online content.

It is important to note that parents typically do not perceive their own child as the ones engaging in risky behaviour. Most parents are more likely to believe that the risks are applicable to other children, and have difficulty in accepting that their own children could behave in similar ways.
Reactions to the use of filters to block access to certain websites were mixed. Some parents perceived that filters on their home computers were effective in protecting their children from exposure to pornography and graphic material. Others had discontinued their use of filters due to the tool blocking access to benign websites, as well as those containing explicit material. Some parents managed the risk of their child being exposed to inappropriate material simply by telling them not to click on ‘pop-ups’ in case they accidentally downloaded a virus.

Overall, most parents recognised their children had the upper hand with social networking services as their children were the ones experienced in their use. Most parents were aware that they could only provide basic advice and knowledge of the risks and that it was the child’s experience of social networking services that would determine whether their child found their advice and these risks relevant or credible.

Children and teenagers were also confident that they knew more than their parents about the risks of the internet, and especially about social networking services. Teenagers were especially aware that their parents had not used social networking services when they were younger, and therefore had no experience from which to draw their knowledge of risks. The internet, and especially social networking, was perceived as unknown territory to parents even by younger children.

“Yeah, Dad doesn’t know nothing.” (eight to nine-year-old girl)

Many parents also claimed they had little knowledge of language their children used to communicate with their friends, with the shorthand used in text messages and social networking services baffling to many parents. Some parents felt it was highly likely that their children had a code to tell friends when their parents were near the computer. They believed that this code was used to tell friends they were interacting with to change subjects quickly, or that they had to log out of the service quickly.

“It is MOD … ‘mother on deck’ … my son does it all the time.”
(Parent of 13 to 17-year-old girl and boy)

11.2 Working together to manage online risks

A range of different parental methods to manage the risks of social networking services were able to be identified. These were often related to the age of children and the parent’s knowledge levels of the risks of social networking services.

Some parents are largely unaware of risks of social networking services. Two different categories have been identified within this group—those who are ‘Totally Trusting’, and ‘Unknowledgeable’. The difference between these two types of parents was the age of their children. Parents typical of the ‘Totally Trusting’ risk management style had teenage children and were unlikely to have ever discussed online risks with their child. These parents had not done so because they were:

> unaware of risks; and/or
> unfamiliar with the internet; and
> unlikely to see the risks as relevant to their child as they believe their child would not engage in risky behaviour.

In contrast, parents in the ‘Unknowledgeable’ style of online risk management typically only had young children aged eight to 12 years. As they had not yet experienced teenage use of the internet, these parents were often unaware of what online risks their children may encounter as they get older simply because they did not see the risks as yet relevant to their child. Once they were made aware that online risks did exist, these parents were often very eager to understand the risks and why they may be relevant to their growing children.
Both of these types of parents would benefit from communication about online risks and the potential online behaviour of children in order to manage these more effectively with their children.

The other types of parents, ‘Realistic Parents’ and ‘Cyber Police’, both have a greater awareness of online risks. These two types of parents differ in how they manage the risks with their children.

‘Realistic Parents’ typically had teenage children. These parents were aware of online risks and tended to assume their child would not follow all the warnings. For example, these parents were more likely to assume that their children:

> had online ‘friends’ they do not know personally; and/or
> viewed explicit or graphic content; and/or
> provided personal details online, albeit in a generalised manner.

‘Realistic Parents’ assist their children manage online risks by taking opportunities to reiterate the risks to their children at appropriate times, such as when their child raises a similar topic in conversation. However, these parents are more likely to be cautious about being perceived as monitoring their children’s behaviour too closely. They were more likely to believe that their child knew more about possible online risk than themselves anyway, and that their key role was to be aware enough to understand should their child have a problem.

Parents typical of the ‘Cyber Police’ risk management style often had children of mixed ages, often with at least one young teenager. These parents perceived themselves as highly aware of their children’s online activities. Most claimed to be highly aware of the online risks, although it was apparent during discussions that some were not. These parents manage online risks with their children by tightly monitoring their activity on services by:

> ensuring they know their child’s password; and/or
> logging on with the child’s identity and checking their child’s profile page and interactions for content; and/or
> checking the computer to see whether their child has erased the recent history of online activity.

Both ‘Realistic Parents’ and ‘Cyber Police’ parents would benefit from communication that reinforces awareness of different online risks and provides strategies of how to manage should problems arise.
12
Communication of online safety messages
Based on the discussion groups and triad interviews, three main sources of internet safety messages were identified. These included schools, parents and websites. Internet safety messages are primarily disseminated through schools. Efforts to communicate internet safety are recognised elsewhere but to a lesser extent, for example via police (through talks in schools), media (news, Channel Nine’s 60 Minutes and A Current Affair) and the government.

“The first time I had heard of Facebook was the other week when they did a feature of it on 60 Minutes.” (Parent of 13 to 15-year-old girl)

12.1 Parents and school messages

Schools are seen as successful in communicating internet safety ‘basics’. The majority of eight to 17-year-olds claimed that internet safety ‘basics’ were taught at school, insofar as not giving out personal details (such as their last name, where they lived, where they went to school, their phone number), as well as alerting them to the risks of ‘stranger danger’. These basics are often communicated either through assembly, by police giving talks at the school or in Personal Development lessons. There is a great deal of repetition throughout primary and high school education, which really embeds the messages in students’ minds. However, repetitious safety messages also have the ability to make students ‘switch off’ if they are seen to be over-stated. Many are familiar with and somewhat complacent about the 40-year-old paedophile posing as a 14-year-old.

“It would have to be a strong message because you are sitting in a hall with all your mates listening to blah, blah, blah.” (16 to 17-year-old boy)

“It is fairly repetitive. They give you examples like this girl got stalked but no-one really pays attention because we know what to do.” (16 to 17-year-old boy)

The evidence suggests that there is a danger this can lead to a lack of understanding of the messages. Over-general messaging might deter children and young people from thinking about the issues, leading them to not understand why some things are potentially risky. For example, not all necessarily understood how giving their last name or password or someone can be risky. Parents do re-enforce the basic internet safety messages and primarily tend to re-iterate the message about predators on the internet.

“I tell my son, remember when you are on Bebo and you tell stories about yourself, then everyone else will do it as well, so not everything there is truthful.”

“I tell him that when he goes on these sex sites that these women are someone’s mother or sister and how would you like your mother or sister to be on something like that. That sort of thing usually makes him think twice.” (Parent of 13-year-old boy)

“I relate the internet to real life. I tell my daughter not to go to the bad parts like […]. Similarly I tell her there are places on the internet she is not meant to go.” (Parent of 10-year-old girl)

Yet many parents admitted they did not feel suitably informed about the internet and the associated risks. Many believed not ‘growing-up’ with the internet puts them at a disadvantage as they had limited internet knowledge and ‘savviness’ which meant that often their children knew more than them. Most parents admitted that they did not ‘actively’ seek information about internet safety, and did not know or want to know about the internet, choosing to believe that schools would provide comprehensive information to ‘fill in the gaps’. Many were unsure when to talk to their children about different internet safety issues, with some not wanting to broach topics like looking at explicit material in fear of giving their children the impetus. Some are unaware when certain issues will begin to affect their children. There is little collaboration between schools and parents as shown in Figure 5.
"I tell him that when he goes on these sex sites that these women are someone's mother or sister and how would you like your mother or sister to be on something like that. That sort of thing usually makes him think twice." (Parent of 13-year-old boy)

"I relate the internet to real life. I tell my daughter not to go to the bad parts like [...]. Similarly I tell her there are places on the internet she is not meant to go." (Parent of 10-year-old girl)

Yet many parents admitted they did not feel suitably informed about the internet and the associated risks. Many believed not 'growing-up' with the internet puts them at a disadvantage as they had limited internet knowledge and 'savviness' which meant that often their children knew more than them. Most parents admitted that they did not 'actively' seek information about internet safety, and did not know or want to know about the internet, choosing to believe that schools would provide comprehensive information to 'fill in the gaps'. Many were unsure when to talk to their children about different internet safety issues, with some not wanting to broach topics like looking at explicit material in fear of giving their children the impetus. Some are unaware when certain issues will begin to affect their children. There is little collaboration between schools and parents as shown in Figure 5.

**Figure 5: How parents and school do and could work together**

<table>
<thead>
<tr>
<th>CURRENT SITUATION</th>
<th>IDEAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>School</td>
<td>School</td>
</tr>
<tr>
<td>Parent</td>
<td>Parent</td>
</tr>
<tr>
<td>Child/ Young person</td>
<td>Child/ Young person</td>
</tr>
</tbody>
</table>

Schools and parents are largely working in isolation

As Figure 5 shows, parents, children and young people have a need for knowledge around the potential risks involved in children using the internet. Schools are a good source of knowledge in this area; however, schools and parents are largely working in isolation. Ideally, schools would have an active role in disseminating information to parents and children. Parents would then use the information to raise their own awareness of online risks, as well as their children’s.

There is a desire for some fresh, ‘real-life’ and engaging communications. There is a belief that communications at present lack new information for older users who do not want to hear repeated storied about a ‘40-year-old paedophile’. They also fail to cover sensitive topics such as suicide, violence and pornography, and the subsequent emotional effects. There is a belief that more true-life stories, similar to news-worthy reports, would help bring the information to life. Current communication is often not in a language or at a level that children and young people can relate to, and fails to reach and impact parents as well as children. There is also little recognition that children and young people have the ultimate responsibility when using these services.

12.2 Website messages

The majority of websites have small clickable links at the bottom displaying their terms and conditions or privacy policy. Children and young people have no desire to click on these links and read the information available as they feel it will not tell them anything they do not already know, as well as often being very text heavy with lots of adult and legal wording. This results in safety messages being largely ignored or missed on social networking services.

Club Penguin and Runescape are relatively effective in communicating a safety message as these explicitly display their safety information on joining the website. While most claim not to read the information, many children and young people could relay the content of these safety messages, for example the age restrictions that apply, being told not to give out personal details, details of behaviour or conduct that will not be tolerated.
Visibly displayed safety information is taken notice of more than an optional link. Club Penguin’s simplicity is successful in getting the safety message getting through, with safety rules popping up as soon as they try to set up a free account, and advice and restrictions against using their first name when naming their penguin. When creating a password, a message to say ‘never share your password’ appears. In addition, parental permission is sought on signing up and a parental review of website is invited if the child is under the age of 13.8

Figure 6: Club Penguin rules

![Club Penguin rules image]

Club Penguin and Runescape are most effective in communicating the safety message, as shown in Figure 7 (below).

Figure 7: Safety messages on social networking services

<table>
<thead>
<tr>
<th>Website</th>
<th>Safety Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Club Penguin (advised 13+)</td>
<td>Parental permission sought</td>
</tr>
<tr>
<td></td>
<td>Simple safety messages/rules displayed on joining</td>
</tr>
<tr>
<td>Runescape (no restriction - conditions)</td>
<td>Unable to relay personal data if under 13 years</td>
</tr>
<tr>
<td></td>
<td>Lengthy terms and conditions but displayed on joining</td>
</tr>
<tr>
<td>Bebo (13+)</td>
<td>Have a safety section at the bottom of their page with videos, animations, parent and teacher advice</td>
</tr>
<tr>
<td></td>
<td>When signing up safety detail is an optional clickable link</td>
</tr>
<tr>
<td>MSN (13+ advised)</td>
<td>Terms of use and privacy statement clickable links on joining</td>
</tr>
<tr>
<td>Facebook (13+)</td>
<td>Terms and privacy are optional clickable links at bottom of page</td>
</tr>
<tr>
<td></td>
<td>On joining terms of use and privacy policy is an optional clickable link</td>
</tr>
<tr>
<td>YouTube (13+)</td>
<td>Safety tips is a clickable link at the bottom of the page</td>
</tr>
<tr>
<td></td>
<td>On joining terms of policy is an optional clickable link</td>
</tr>
<tr>
<td>MySpace (14+)</td>
<td>Safety tips link at bottom of webpage</td>
</tr>
<tr>
<td></td>
<td>On joining ‘terms of service ’ is an optional link</td>
</tr>
</tbody>
</table>

---

8 These sites request an email address of a parent for this purpose. However, this does not mean that parents will always legitimately provide their permission. Such procedures are open to abuse, for example, where emails are intercepted prior to being received by parents. Please note, no evidence of this was found in the research.
13
Conclusions and recommendations
13.1 Conclusions

Amongst young people, there is high awareness of the obvious risks of online use, such as the dangers posed by predators and the risk of cyberbullying. These are taught from a very young age and are delivered via a range of communications channels such as school and parents. Yet some young people are still engaging in the behaviour and it is seen as the ‘norm’ in that everyone appears to be doing it to some extent. Exploring the unknown and pushing the boundaries is a natural part of growing up. To many, the internet and social networking services are very much seen as still part of a game; it is not the real world. Therefore the risks are not real either.

The perception of the likelihood that risks will become reality is largely based on experience. There is an obvious disconnect between what young people are told is high risk behaviour in relation to social networking services, and what they perceive as being high risk in their actual use of the services, due to the risks not eventuating in many cases. Experience of the services does not lead to many finding the stated risks as credible, for example their experience of the ‘predator’, which is the risk widely seen as the greatest threat to young people, is very limited. The experience of girls suggested that some form of cyberbullying was common behaviour and experienced on social networking services but there were noticeable differences in how various girls dealt with the situations.

Most parents have a lack of knowledge about their children’s actual behaviour, the internet in general; and the risks involved using a social networking service beyond that of the ‘predator’. Most parents will not typically seek out information on online risks.

13.2 Recommendations

1/ Communications about risks for young people can be made more engaging both in content and in delivery.

2/ For children (aged eight to 12) there is potential to educate through use of a website. This will be more engaging for children if it is as entertaining as the games they play:
   > interactive, for example make the quiz on safety more of a game;
   > uses videos and characters rather than text;
   > uses the language of children, not adults.

3/ Content for late teens should be ‘in language’, however it must be recognised that this changes quickly. For example, in some of the group discussions ‘strangers’ were referred to as ‘randoms’, which may no longer be the common vernacular. It will be important to test content of any produced information with young people in order to refine language and ensure it is relevant to the target audience.
4/ In terms of content, late teens should be provided with new information, other than the risk of the 40-year-old predator. Some information that the different segments may find relevant include:

> for ‘Active Risk-takers’ and ‘Responsible Risk-takers’, the adding up of disparate pieces of personal information an individual chooses to give out.

> for the ‘Vulnerably Influenced’ highlighting that situations do get out of control, for example the risks of meeting someone in person and cyberbullying. In addition, emphasising that assistance is available in this situation.

> amongst ‘Specialist Seekers’ ensuring that they consider that risks, even that of the predator, are as applicable to special interest forums as they are to general social networking services.

> amongst ‘Claimed Conformists’ reinforcing the positive behaviour.

5/ There is a need to consider non-traditional delivery channels for young people. Alternative channels of communication that involve young people, rather than offering them information in a didactic manner are likely to be more effective as they:

> recognise that young people feel that they are more knowledgeable about these websites than parents/teachers;

> place responsibility on the young person.

6/ Workshop approaches could be potentially effective as they place participants on a more equal level as the facilitator. Young people can be encouraged to discuss personally relevant issues in response to the broader topics, sharing their experiences and behaviours without fear of punishment. In addition, interactivity through games or role-play could also provide experience of the known theory. For example mimicking a situation where disparate pieces of information are added up based on what a young person claims they would provide to others online.

7/ Capitalise on the natural teenage curiosity of the unknown. Shock communications can be used but will be more effective if they involve real life stories.

8/ Greater collaboration between parents and schools will assist in increasing parental knowledge and address the fact that most parents will not actively seek out information.

9/ Information aimed at parents could include education on what social networking services are, typical behaviour of young people on the services, potential risks exist beyond that of the predator, and a jargon buster.
Appendix A

Screeners
APPENDIX A: RECRUITMENT SCREENER

13-17 year old focus groups/bulletin board participants

JOB NUMBER: J2800

PROJECT: ACMA Cybersafety

RESEARCHER (S): Amy Hibbert, Victoria Parr, Kees Van Duyn

INTRODUCTION

Good morning/afternoon/evening, my name is ________________ and I am calling on behalf of an independent market research company called GfK Blue Moon. We are currently conducting some research for the Australian Communications and Media Authority about online behaviour and are looking for people to take part in either an online bulletin board or face to face discussion group or both. Would this be something that you would be interested in?

We are looking for people that fit a certain criteria, so I would need to ask you some questions initially to see if you are who we need for this research. Would you have a few spare minutes to answer some questions for me?

Firstly, before I ask you anything, could I please talk to either your parent or guardian to check they are happy for me to talk to you?

PLEASE ENSURE THAT YOU GAIN PERMISSION FROM A PARENT OR GUARDIAN BEFORE YOU PROCEED. REASSURE THEM THAT OUR RESEARCHERS WILL NOT EXPOSE THEIR CHILDREN TO ANY UNSUITABLE MATERIAL OR PUT THEM AT ANY RISK. AS RESEARCHERS WE ARE BOUND BY A STRICT CODE OF CONDUCT SET BY THE MARKET RESEARCH SOCIETY OF AUSTRALIA.

IF RESPONDENTS WISH TO VERIFY THE RESEARCH THEY CAN CONTACT EITHER AMY HIBBERT AT GFK BLUE MOON: (02) 9460 6555 OR MATTHEW DOBSON AT AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY: (02) 9334 7883

Q1 ASK PARENT

1. What is the current occupation of all household members? (RECORD)

AIM FOR A MIX.
DO NOT RECRUIT ANYONE WHO MENTIONS MARKETING / RESEARCH / ADVERTISING / MEDIA.

REMAINDER OF QUESTIONS ASK YOUNG PERSON

2. Have you taken part in a market research discussion group before?

| GO TO Q3 --- | Yes | 1 |
3. How many times have you taken part in a market research discussion group?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3+</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DO NOT RECRUIT ---</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. Have you taken part in a market research discussion group in the last 6 months?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DO NOT RECRUIT ---</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. Do you have internet access at home?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DO NOT RECRUIT ---</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. How often do you use the internet for anything other than school related activities? **READ OUT**

<table>
<thead>
<tr>
<th>Daily</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-6 times a week</td>
<td>2</td>
</tr>
<tr>
<td>2-3 times a week</td>
<td>3</td>
</tr>
<tr>
<td>Once a week</td>
<td>4</td>
</tr>
<tr>
<td><strong>DO NOT RECRUIT ---</strong></td>
<td></td>
</tr>
<tr>
<td>Less than once a week</td>
<td>5</td>
</tr>
</tbody>
</table>

7. A) Which of the following websites have you visited in the last month? **READ OUT**
   B) Which 3 do you visit most often?

<table>
<thead>
<tr>
<th>Website</th>
<th>Visited in last month</th>
<th>3 most frequent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bebo</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Club Penguin</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>facebook</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Flixter</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Friends Reunited</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Habbo</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>imvu</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>MySpace</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>Twitter</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>Windows Live Spaces (formerly MSN Spaces)</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Xanga</td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Yahoo! 360</td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>You Tube</td>
<td></td>
<td>13</td>
</tr>
<tr>
<td>Other websites that involve chat, profiles, social activities, virtual gaming worlds please specify:</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td><strong>DO NOT RECRUIT ---</strong></td>
<td>None of the above</td>
<td>15</td>
</tr>
</tbody>
</table>
8. Which of the following would you ever do online?

<table>
<thead>
<tr>
<th>AIM FOR A MIX</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post a photo of yourself</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Provide your real name, if someone asked you to</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Provide your phone number to someone if they asked you to</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Arrange to meet someone in person who you had first met online</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>None of the above</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

9. Which academic year are you in at high school?

<table>
<thead>
<tr>
<th>CHECK QUOTA ---</th>
<th>Year 8</th>
<th>Year 9</th>
<th>Year 10</th>
<th>Year 11</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

10. Do you have any disabilities at all?

<table>
<thead>
<tr>
<th>Yes, please specify</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, please specify</td>
<td>1</td>
</tr>
<tr>
<td>No</td>
<td>2</td>
</tr>
</tbody>
</table>

**RECORD GENDER:**

<table>
<thead>
<tr>
<th>AIM FOR MIX</th>
<th>Male</th>
<th>Female</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

**RECORD EMAIL ADDRESS:**


**PREFERRED USERNAME FOR DISCUSSION BOARD:**


RECRUITMENT SCREENER
Parent Groups

JOB NUMBER: J2800
PROJECT: ACMA Cybersafety
RESEARCHER (S): Amy Hibbert, Victoria Parr

INTRODUCTION

Good morning/afternoon/evening, my name is ________________ and I am calling on behalf of an independent market research company called GfK Blue Moon. We are currently conducting some research for the Australian Communications and Media Authority about young people’s online behaviour and wish to speak to parents face to face in a group discussion. Would this be something that you would be interested in?

We are looking for people that fit a certain criteria, so I would need to ask you some questions initially to see if you are who we need for this research. Would you have a few spare minutes to answer some questions for me?

IF RESPONDENTS WISH TO VERIFY THE RESEARCH THEY CAN CONTACT EITHER AMY HIBBERT AT GFK BLUE MOON: (02) 9460 6555 OR MATTHEW DOBSON AT AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY: (02) 9334 7883

11. What is the current occupation of all household members? (RECORD)

AIM FOR A MIX.
DO NOT RECRUIT ANYONE WHO MENTIONS MARKETING / RESEARCH / ADVERTISING / MEDIA.

12. Have you taken part in a market research discussion group before?

<table>
<thead>
<tr>
<th>GO TO Q3 ---</th>
<th>Yes</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>GO TO Q5 ---</td>
<td>No</td>
<td>2</td>
</tr>
</tbody>
</table>

13. How many times have you taken part in a market research discussion group?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>DO NOT RECRUIT ---</td>
<td>3+</td>
<td>3</td>
</tr>
</tbody>
</table>

14. Have you taken part in a market research discussion group in the last 6 months?

<table>
<thead>
<tr>
<th>DO NOT RECRUIT ---</th>
<th>Yes</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>2</td>
</tr>
</tbody>
</table>
15. Do you have a child of high school age living at home, that currently accesses the internet for activities other than school study?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do Not Recruit ---</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

16. How often do your child use the internet for anything other than school related activities? **READ OUT**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Daily</th>
<th>4-6 times a week</th>
<th>2-3 times a week</th>
<th>Once a week</th>
<th>Less than once a week</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AIM FOR A MIX ---</strong></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td><strong>Do Not Recruit ---</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

17. Which academic year is your child in at high school?

<table>
<thead>
<tr>
<th>Year</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AIM FOR A MIX ---</strong></td>
<td>Year 8</td>
</tr>
<tr>
<td>Year 8</td>
<td>1</td>
</tr>
<tr>
<td>Year 9</td>
<td>2</td>
</tr>
<tr>
<td>Year 10</td>
<td>3</td>
</tr>
<tr>
<td>Year 11</td>
<td>4</td>
</tr>
</tbody>
</table>

18. Which of the following best describes your level of awareness of what your child is looking at on the internet?

<table>
<thead>
<tr>
<th>Description</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AIM FOR A MIX ---</strong></td>
<td></td>
</tr>
<tr>
<td>I constantly oversee and sensor websites my child looks at</td>
<td>1</td>
</tr>
<tr>
<td>I occasionally have a look at the websites my child is looking at</td>
<td>2</td>
</tr>
<tr>
<td>I check the search history on our computer to see which websites my child has been looking at</td>
<td>3</td>
</tr>
<tr>
<td>I talk to my child about websites they look at but have not seen them myself</td>
<td>4</td>
</tr>
<tr>
<td>I wouldn’t have a clue what websites my child looks at</td>
<td>5</td>
</tr>
</tbody>
</table>

**RECORD GENDER:**

<table>
<thead>
<tr>
<th>Gender</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AIM FOR MIX</strong></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>1</td>
</tr>
<tr>
<td>Female</td>
<td>2</td>
</tr>
</tbody>
</table>
RECRUITMENT SCREENER
8-12 year old in-home triads with parents

JOB NUMBER: J2800

PROJECT: ACMA Cybersafety

RESEARCHER (S): Amy Hibbert, Victoria Parr, Kees Van Duyn

INTRODUCTION

Good morning/afternoon/evening, my name is ________________ and I am calling on behalf of an independent market research company called GfK Blue Moon. We are currently conducting some research for the Australian Communications and Media Authority about online behaviour and are looking for young people and their parents to take part in a face to face discussion held at your home. Would this be something that you would be interested in?

We are looking for people that fit a certain criteria, so I would need to ask you some questions initially to see if you are who we need for this research. Would you have a few spare minutes to answer some questions for me?

REASSURE THEM THAT OUR RESEARCHERS WILL NOT EXPOSE THEIR CHILDREN TO ANY UNSUITABLE MATERIAL OR PUT THEM AT ANY RISK. AS RESEARCHERS WE ARE BOUND BY A STRICT CODE OF CONDUCT SET BY THE MARKET RESEARCH SOCIETY OF AUSTRALIA.

IF RESPONDENTS WISH TO VERIFY THE RESEARCH THEY CAN CONTACT EITHER AMY HIBBERT AT GFK BLUE MOON: (02) 9460 6555 OR MATTHEW DOBSON AT AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY: (02) 9334 7883.

PLEASE MAKE SURE EVERY PARENT AND YOUNG PERSON IS SCREENED AND FITS THE CRITERIA.

19. What is the current occupation of all household members? (RECORD)

AIM FOR A MIX.
DO NOT RECRUIT ANYONE WHO MENTIONS MARKETING / RESEARCH / ADVERTISING / MEDIA.

QUESTIONS 2-5 TO BE ASKED OF BOTH YOUNG PEOPLE AND PARENTS

20. Have you taken part in a market research discussion group before?

<table>
<thead>
<tr>
<th>GO TO Q3 ---</th>
<th>Yes</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>GO TO Q5 ---</td>
<td>No</td>
<td>2</td>
</tr>
</tbody>
</table>
21. How many times have you taken part in a market research discussion group?

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3+</th>
</tr>
</thead>
<tbody>
<tr>
<td>DO NOT RECRUIT ---</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

22. Have you taken part in a market research discussion group in the last 6 months?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>DO NOT RECRUIT ---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

23. Do you have internet access at home?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>DO NOT RECRUIT ---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PARENTS GO TO Q10**

**QUESTIONS 6-10 TO BE ASKED OF YOUNG PEOPLE ONLY**

24. How often do you use the internet for anything other than school related activities? **READ OUT**

<table>
<thead>
<tr>
<th></th>
<th>Daily</th>
<th>4-6 times a week</th>
<th>2-3 times a week</th>
<th>Once a week</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIM FOR A MIX ---</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>DO NOT RECRUIT ---</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

25. A) Which of the following websites have you visited in the last month? **READ OUT**

B) Which 3 do you visit most often?

<table>
<thead>
<tr>
<th>visiting websites in last month</th>
<th>3 most frequent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bebo</td>
<td>1</td>
</tr>
<tr>
<td>Club Penguin</td>
<td>2</td>
</tr>
<tr>
<td>facebook</td>
<td>3</td>
</tr>
<tr>
<td>Flixtor</td>
<td>4</td>
</tr>
<tr>
<td>Friends Reunited</td>
<td>5</td>
</tr>
<tr>
<td>Habbo</td>
<td>6</td>
</tr>
<tr>
<td>imvu</td>
<td>7</td>
</tr>
<tr>
<td>MySpace</td>
<td>8</td>
</tr>
<tr>
<td>Twitter</td>
<td>9</td>
</tr>
<tr>
<td>Windows Live Spaces (formerly MSN Spaces)</td>
<td>10</td>
</tr>
<tr>
<td>Xanga</td>
<td>11</td>
</tr>
<tr>
<td>Yahoo! 360</td>
<td>12</td>
</tr>
<tr>
<td>You Tube</td>
<td>13</td>
</tr>
</tbody>
</table>

**MUST VISIT AT LEAST 1 ---**

Other websites that involve chat, profiles, social activities, virtual gaming worlds please specify:

<table>
<thead>
<tr>
<th></th>
<th>Visited in last month</th>
<th>3 most frequent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
26. Which academic year are you in at primary school?

<table>
<thead>
<tr>
<th>CHECK QUOTA ---</th>
<th>Year 3</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Year 4</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Year 5</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Year 6</td>
<td>4</td>
</tr>
</tbody>
</table>

27. Do you have any disabilities at all?

<table>
<thead>
<tr>
<th></th>
<th>Yes, please specify</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>2</td>
</tr>
</tbody>
</table>

PARENTS ONLY

28. Which of the following best describes your level of awareness of what your child is looking at on the internet?

<table>
<thead>
<tr>
<th>AIM FOR A MIX ---</th>
<th>I constantly oversee and sensor websites my child looks at</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>I occasionally have a look at the websites my child is looking at</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>I check the search history on our computer to see which websites my child has been looking at</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>I talk to my child about websites they look at but have not seen them myself</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>I wouldn’t have a clue what websites my child looks at</td>
<td>5</td>
</tr>
</tbody>
</table>

RECORD GENDER:

<table>
<thead>
<tr>
<th>AIM FOR MIX</th>
<th>Male</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Female</td>
<td>2</td>
</tr>
</tbody>
</table>
Appendix B
Discussion guides
APPENDIX B: DISCUSSION GUIDE

Triads - 8-12 year olds
1 hour

<table>
<thead>
<tr>
<th></th>
<th>Introduction</th>
<th>5 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>• Moderator describes nature and purpose of research – online behaviour</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Respondents introduce themselves, i.e., school year, siblings’ ages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• What do you like to do in your spare time?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Online Behaviour general</th>
<th>5 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>• When did you first start going online?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• How much time do you spend online?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• How much is that compared to other activities?</td>
<td></td>
</tr>
</tbody>
</table>

**Self Complete Exercise 1:** respondents divide a pie-chart according to time spent on different online activities

<table>
<thead>
<tr>
<th></th>
<th>Accompanied Online Surf</th>
<th>25 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><strong>Ask respondents to show you what they normally do when they go online, making sure each has an equal amount of time on the computer.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Ask them to specifically show examples of the following:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Which sites are your favourite?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• What do you like about this site?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• What stands out/appeals?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• What do you dislike about this site?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• What do you do on these sites?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• How has what you do on the internet changed at all over the past 6 months?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Which were/are your favourite sites &amp; which are you spending more/less time on?</td>
<td></td>
</tr>
</tbody>
</table>
If not already shown, ask respondent to show you a site that they particularly like that allows them to communicate with other people online

- What do you call these types of sites?
- What do you use them for?
- How important is being able to (activities that they do on the sites) to you? Why?
- Which of these activities are more / less important to you?
- What’s not so good about these sites?
- Do you ask your Mum and Dad for permission to access these sites? (Follow-up as required: Would your Mum and Dad know that you access these sites?)
- Are you aware of the age limits that apply to people who access certain sites on the internet?
  - Which sites?
- What do they think about having to be a certain age to gain access to some sites?
- Do you know where to look on these sites for safety information?
- Have you ever access the safety information on these sites?

Moderator to note any spontaneous mentions of contact, privacy and content issues and to probe
- What do you mean by that?
- How often does that happen?

Self Complete Exercise 2: Joining Bebo under age of 13 yrs

N.B. If respondents mention relationships or sharing information online probe with some questions on contact and privacy from teenagers guide, otherwise do not broach the topics and focus on content

Ask respondents to think about the types of material/content they come across online

Self Complete Exercise 3 – Scenario on settings/filters
- Does your family have any rules about how long you can be online?
- Does your family have any rules about what type of content you can access online?
- Have your or anyone you know’s parents placed any filters or controls on what they can access on the internet?
- What do you think about this?
- Have you ever come across anything online that you think is gross? What?

Moderator to note
- Do you ever come across anything online that you know your parents wouldn’t want you looking at? What?
Moderator to note
- What types of site would have these things on it?
- How often would you come across these things by accident?
- What do you normally do in this type of situation?

6 Online Safety

- What are some of your concerns about being online?
- Have you or anyone you know ever come across anything that you would consider risky on the internet? What? What did you do?
- Have you ever been given information or been told about online risks?
  - Who/where from?
- Do you think your parents know what they are on about in regards to what you do online?
  - Why/why not?

7 Reactions to existing Cybersafety Materials

Show Cybersmart website pages


- Have you ever seen this type of material before?
- What do you think of it?
- What do you like about these?
- What do you not like about these?

8 Summing Up

- What do they think will be the next most popular things to do online?
- What do you think you will be doing on the internet in a few year’s time?
- If you had to design a website like those we’ve shown you what would you put in it to make it appeal to people your age?
- What do you think is the most important thing to have on a website to make it appeal to people your age?
## DISCUSSION GUIDE

Up to 1 ¾ hours

<table>
<thead>
<tr>
<th></th>
<th>Introduction</th>
<th>5 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Moderator describes nature and purpose of research – their children’s online behaviour</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Respondents introduce themselves, i.e., kids, occupation etc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Children’s Online Behaviour</th>
<th>10 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>How much time do your children spend online?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>How much is that compared to other activities?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What do you think your children are doing while online? <em>Moderator to make a list</em></td>
<td></td>
</tr>
</tbody>
</table>

**Self Complete Exercise 1:** respondents divide a pie-chart according to time their children spend on different online activities

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Do you know if what your children do online has changed at all over the past 6 months?</td>
</tr>
<tr>
<td></td>
<td>Which are some of your children’s favourite sites?</td>
</tr>
<tr>
<td></td>
<td>Which sites do they spend more/less time on?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Social Networking Sites</th>
<th>10 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>Moderator to show group list of the social networking site mentioned so far</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>What do you think about these sites as a group?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What do your children use them for?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Why do your children like them?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>How important is being able to (activities that they do on the sites) to you children? Why?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What don’t you like about your children using these sites?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Do you ever have any concerns about your children using these sites? What?</td>
<td></td>
</tr>
</tbody>
</table>

**Moderator to note any spontaneous mentions of contact, privacy and content issues and to probe**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>What do you mean by that?</td>
</tr>
<tr>
<td></td>
<td>Why does that concern you?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Online Relationships (Contact)</th>
<th>15 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>What’s different about the relationships or friend or contacts your children have online compared to those in real life?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Do they differ at all? Are your children friends with different groups of people online?</td>
<td></td>
</tr>
</tbody>
</table>
• What is good about your children having friendships/relationships online?
• What’s not so good?
• Do you think your children ever go too far when talking to each other online?
• What’s too far in your minds?
• In your opinion, what is cyberbullying?
• Have you ever talked to your children about cyberbullying?
• Have you ever seen any evidence of cyberbullying?
• Do you ever talk to your children about who they are talking to online?
• Have you ever heard about any children meeting up with people face-to-face who they’ve met online?
  – Have you ever talked to your children about this?
  – If so what did you say?
  – How did they respond?
• Do you have any other concerns about your children’s online relationships?

5 Sharing of Information/online material (privacy) 15 minutes

• What type of information do your children upload about themselves?
• What would your children upload to their favourite (social networking) site?
• What do you think about your children sharing this type of information online with people?
  – What are the positives? Do you have any concerns?
• Do you ever see what other children have uploaded?
  – What do you think about that?
• Do you ever think about your childrens’ digital footprint (the information they upload and is a record for other people to access or have in the future)?
• What do you think about your children giving people who they don’t know personally......online?
  – Photo
  – Real name
  – Phone number
  – School location
  – Home address
• Have you ever heard about any children doing this?
• Have you ever talked to your children about what information they should/shouldn’t give online?
  – If so what have you said?
  – How have they responded?

6 Online Material (Content) 15 minutes

Ask respondents to think about the types of material/content their children may come across online

• Have your got any filters or controls on what your children can access on the internet?
  – Why did you decide to/not to?
If not, have you ever considered it? What would your children say/do?
If have, what do your children think about it?
• What material do you specifically worry about your children accessing online? Why?

**Moderator to note on a list**
• Which sites/type of sites would have this material on it?
• How often do you think your children come across these things by accident?
• Do you ever think they would search them out?
• What do you think your children do in these situations? Honestly?
• Have you ever talked to your children about what is inappropriate material/content?
  – What kind of content have you discussed?
  – What have you said?
  – How have they responded?

### 7 Online Safety 15 minutes

• What other concerns do you have about your children’s online activities?
• Is there a difference between what you think is risky and what your children think is risky?
• Where do you get your information about what types of risks there are online for children?
  o Probe media, government, children, other parents, schools, ISPs, the privacy guidelines on social networking sites, other places?
• What type of information do you get from these places?
• (if not already covered) Do you ever talk about social networking sites specifically with your children?
  – Who starts the conversation? You or them?
• Do you think you have a good grasp of what your children do online?
  – Why/ why not?
• What information do you want to know about:
  – social networking sites?
  – what’s risky online/what’s not?
• What don’t you know that you think you should?

### 8 Reactions to Existing Cybersafety Materials 10 minutes

*Show Cybersmart website pages*


- Have you ever seen this type of material before?
- What do you think of it?
- What do you like about these?
- What do you not like about these?

**Show excerpt from ACMA 'Wise up to IT' clips (appropriate to age/gender)**
- Have you ever seen this type of material before?
- What do you think of it?
- What do you like about these?
- What do you not like about these?

<table>
<thead>
<tr>
<th>9</th>
<th>Summing Up</th>
<th>5 minutes</th>
</tr>
</thead>
</table>

- If you were designing information about online risks aimed at young people, what would be the key topics/messages?
- Where would you put it so children would take notice of it?
- Who would that information need to come from?
DISCUSSION GUIDE
Up to 1 ¾ hours

Homework/Bulletin Board Questions

- About them and their family?
- What do you like about the internet?
- What are your favourite websites?
- Why do you like these sites? What is it about them?
- Is there anything you don’t like about the websites – especially the social networking sites?
- What do people talk about? Post on the internet?

1 Introduction

- Moderator describes nature and purpose of research – online behaviour
- Respondents introduce themselves, i.e., school year, siblings’ ages
- What do you like to do in your spare time?

2 Review of Homework Questions (bulletin board respondents only)

Moderator to pick out some key conversation points from the bulletin board

- What is good about some of the sites you visit?
- Is there anything you don’t like about the websites – especially the social networking sites?
  - What do people talk about/post on the internet?
- Did anything surprise you about any comments that were made by others?

3 Online Behaviour

- How much time do you spend online?
- How much is that compared to other activities?
- What do you do when you are online? Moderator to make a list
- Do you ever use a webcam when you are talking to people online?
  - Who do you use it with?

Self Complete Exercise 1: respondents divide a pie-chart according to time spent on different online activities

- How has what you do on the internet changed at all over the past 6 months?
- Which were/are your favourite sites? & which sites are you spending more/less time on?
Social Networking Sites

Moderator to show group list of the social networking sites mentioned so far

• What do you call these types of sites?
• What do you think about these sites as a group?
• What do you use them for?
• How important is being able to (activities that they do on the sites) to you? Why?
• Which of these activities are more / less important to you?
• What’s not so good about these sites?

Moderator to note any spontaneous mentions of contact, privacy and content issues and to probe

• What do you mean by that?
• How often does that happen?

Online Relationships (Contact)

• What’s different about the relationships or friend or contacts you have online compared to those in real life?
• Do they differ at all? Are you friends with different groups of people online?
• Do you talk about different things with different groups of people online?
• What is good about online relationships?
• What’s not so good?
• Do people ever go too far when talking to each other online?
• What’s too far in your minds?

Self Complete Exercise 2– Scenario on cyberbullying

• Do you know or have you heard about anyone that that sort of thing has happened to?
• Do you know or have you heard about anyone who has done that sort of thing before?
• If yes, how have they done it?
  – SMS
  – IM
  – Web-based
  – flames
  – fake profile
• Have you or anyone you know ever used a webcam with someone you don’t know personally? Why would you/ wouldn’t you do this?
• Do people ever meet up with people face-to-face who they have met online?
• Have you or do you know anyone who has been asked to meet up with people face-to-face who you’ve met online?
  – Would you do this? Why/why not?
  – If you were to do this/know someone who has done this, would you take anyone with you? Who?

6 Sharing of Information/online material (privacy) 15 minutes

• What type of information do people your age upload about yourselves?
• What would you upload to your favourite (social networking) site?
• What types of information/material do other people your age upload?
  – What do you think about that?
• What’s good about sharing this type of information online with people?
• What’s not so good to share with people online, that you might have seen others share?
• Do you ever think about what people might say in the future about what you upload?
• What do you think about giving people who you don’t know personally……online?
  – Photo
  – Real name
  – Phone number
  – School location
  – Home address
• Do you know anyone who has done this?

7 Online Material (Content) 15 minutes

Ask respondents to think about the types of material/content they come across online

Self Complete Exercise 3 – Scenario on settings/filters

• Have your or anyone you know’s parents placed any filters or controls on what they can access on the internet?
• What do you think about this?
• Have you ever come across anything online that you think is gross? What?
  
Moderator to note on a list

Do you ever come across anything online that you know your parents wouldn’t want you looking at? What?

Moderator to note on a list

• What types of site would have these things on it?
• How often would you ‘accidentally’ come across these things?
• What do you normally do in this type of situation?
**Self Complete Exercise 4 - Scenario giving info/meeting someone (age appropriate)**

**Discuss reactions to different parts of the scenario**

- Why do you not think that part is risky (e.g. phone number) and the other part is (e.g. going over to a house)
- What do you see as the difference in riskiness between them?
- Do you know anyone who might respond differently?
- What examples can you give of something you or someone you know has done that is risky?
  - Why is that a risk?
  - Do you try and manage/reduce the risks? How? Does it depend who is around when you are online?
- Is there a difference between what you think is risky and what others tell you is risky, like your parents?
- Where do you get your information on about what types of risks there are online?
  - Probe with media, government, friends, parents, school, ISPs? The privacy guidelines on social networking sites? Other places?
- What type of information do you get from these places?
- Do you ever talk about (social networking) sites with your parents?
- Who starts the conversation? You or your parents?
- Do you think your parents know what they are on about in regards to what you do online?
  - Why/ why not?
- What do you think your parents need to know about social networking sites, and what’s risky online and what’s not?

**Reactions to existing Cybersafety Materials**

**Show Cybersmart website pages**


• Have you ever seen this type of material before?
• What do you think of it?
• What do you like about these?
• What do you not like about these?

Show excerpt from ACMA ‘Wise up to IT’ clips (appropriate to age/gender)
• Have you ever seen this type of material before?
• What do you think of it?
• What do you like about these?
• What do you not like about these?
• How could they better appeal to you?

10 Summing Up

• What do they think will be the next most popular things to do online?
• If you were designing information about online risks aimed at young people like you or for people in your parents age group
• What would be the key topics/messages covered?
• Where would you take notice of information that tells you about some of the risks online?
• Who would that information need to come from?
Appendix C
Using this research
It is important that clients should be aware of the limitations of survey research.

**Qualitative research**

Qualitative research deals with relatively small numbers of respondents and attempts to explore in-depth motivations, attitudes and feelings. This approach places a considerable interpretative burden on the researcher. For example, often what respondents do not say is as important as what they do say. Similarly, body language and tone of voice can be important contributors to understanding respondents’ deeper feelings.

Client should therefore recognise:

> that despite the efforts made in recruitment, respondents may not always be totally representative of the target audience concerned; and

> that findings are interpretative in nature, based on the experience and expertise of the researchers concerned.

**Quantitative research**

Even though quantitative research typically deals with larger numbers of respondents, users of survey results should be conscious of the limitations of all sample survey techniques.

Sampling techniques, the level of refusals, and problems with non-contacts all impact on the statistical reliability that can be attached to results.

Similarly, quantitative research is often limited in the number of variables it covers, with important variables beyond the scope of the survey.

Hence the results of sample surveys are usually best treated as a means of looking at the relative merits of different approaches as opposed to absolute measures of expected outcomes.

**The role of researcher and client**

Blue Moon believes that the researchers’ task is not only to present the findings of the research but also to utilise our experience and expertise to interpret these findings for clients and to make our recommendations (based on that interpretation and our knowledge of the market) as to what we believe to be the optimum actions to be taken in the circumstances: indeed this is what we believe clients seek when they hire our services. Such interpretations and recommendations are presented in good faith, but we make no claim to be infallible.

Clients should, therefore, review the findings and recommendations in the light of their own experience and knowledge of the market and base their actions accordingly.
**avatar**: A computer user’s graphical representation of him or herself. An avatar can be two or three-dimensional.

**Bebo**: A social networking website, founded in 2005.

**blog**: Blog is short for weblog. A weblog is a series of entries arranged in reverse chronological order, often updated on frequently with new information about particular topics.

**chatrooms**: An online area where users can chat with other users in real time.

**closed game websites**: Games websites that involve only one player.

**Club Penguin**: An online games website that uses penguins as avatars. The website was founded in 2005.

**cyberbullying**: The use of information and communication technologies, such as email, mobile phone and pager text messages, instant messaging (IM) and defamatory personal websites to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others. Note, however, that this term was not explicitly defined for focus group participants in this qualitative study.

**cybersafety**: A term used to describe user safety while online.

**diary sites**: An alternative term used to describe websites containing weblogs.

**Facebook**: A social networking website founded in 2004.

**forum**: An online area for holding discussions and posting content.

**friend**: Anyone who accepts an invitation from another social networking site user to be friends.

**Habbo (or the Habbo Hotel)**: A social networking website that is aimed at teenagers and is based around virtual hotel rooms. Each user has a customisable avatar to represent them.

**Instant messaging**: An online service that allows users to ‘chat’ via text messages in real time with one another.

**LimeWire**: A website that users can share files with one another.

**multiplayer sites**: An online computer game which is capable of supporting hundreds or thousands of players simultaneously. Examples include Club Penguin, Runescape and World of Warcraft.

**MSN messenger**: An instant messaging service, first developed by Microsoft in 1999 and renamed in 2006 as Windows Live Messenger.

**MySpace**: A social networking site founded in 2003.

**open game websites**: Games websites that involve more than one player.

**pop-up**: A small window that appears (pops-up) over a webpage.

**profile**: The personal homepage on a social networking site, usually including information about a user, photographs, and their friend list. Profiles form the basis of social networking websites.

**randoms**: A term used to describe strangers that a user may come into contact with online.

skin(s): The background or texture of a user’s profile, which may include patterns, animations, photos and other formatting. Skins are commonly found on social networking sites.

Skype: A software programme that allows users to make telephone calls over the internet, using VOIP (voice over internet protocol) technology.

social networking website: A website that allows users to create a personal page or profile and construct and display a social network of their online contacts.

stranger danger: Describes the possible danger presented to children by strangers.

user-generated websites: Websites essentially made up with content provided by users, such as photographs, blog entries and videos.

webcam: A small camera attached to or built into a computer, which relays images online.

World of Warcraft: A multi-player online role-player game founded in 1994.

YouTube: A popular video sharing website founded in 2005.