Teenagers, Legal Risks and Social Networking Sites

Melissa de Zwart
David Lindsay
Michael Henderson
Michael Phillips
This publication has been supported with a General Grant from the Victoria Law Foundation. Website: www.victorialawfoundation.org.au

Title: Teenagers, Legal Risks and Social Networking Sites
Authors: Melissa de Zwart
         David Lindsay
         Michael Henderson
         Michael Phillips

ISBN: 978-0-646-55345-0

Published by: Monash University
              Faculty of Education
              Building 6
              Monash University
              Victoria 3800
              Australia
              Phone: +61 3 99052868
              Email: michael.henderson@monash.edu

© Melissa de Zwart, David Lindsay, Michael Henderson and Michael Phillips. 2011.

This work is copyright. It may be reproduced in whole or in part for study or training purposes subject to the inclusion of an acknowledgement of the source and no commercial usage or sale. It may also be reproduced for purposes permitted by the Copyright Act 1968 (Cth). Reproduction for purposes other than those indicated above may be made with the permission of the authors.
# Table of Contents

Table of Contents............................................................................................................................. iii  
List of Tables..................................................................................................................................... v  
List of Figures................................................................................................................................... vi  
Acknowledgements ........................................................................................................................ vii  
Authors.......................................................................................................................................... viii  
1. Executive Summary ..................................................................................................................... 1  
1.1. Key findings ......................................................................................................................... 1  
1.2. Key recommendations ......................................................................................................... 3  
1.3. Publications .......................................................................................................................... 4  
1.4. Structure of the Report ......................................................................................................... 5  
2. Introduction ................................................................................................................................. 6  
2.1. Project background ............................................................................................................... 6  
2.2. Scope of the project ............................................................................................................. 7  
2.3. Benefits and risks of SNS ................................................................................................. 9  
2.4. What are the legal risks? ................................................................................................. 11  
2.5. Summary ............................................................................................................................ 17  
3. Research Design: Student SNS practices and perceptions of legal risk............................... 18  
3.1. The participants ................................................................................................................ 19  
3.2. Surveys ............................................................................................................................. 22  
3.3. Interviews ......................................................................................................................... 22  
3.4. Data Analysis ................................................................................................................... 23  
4. Results: Student SNS practices and perceptions of legal risk ............................................ 24  
4.1. The number of middle school students’ using SNS ......................................................... 24  
4.2. Specific SNS used by middle school students .................................................................. 26  
4.3. Frequency of middle phase students using SNSs ............................................................ 28  
4.4. What students do with SNS ............................................................................................ 31  
4.5. The content which students post to SNS ....................................................................... 37  
4.6. The value of SNS .............................................................................................................. 44  
4.7. Perceptions of risk .......................................................................................................... 47  
4.8. Teachers’ use of SNS ....................................................................................................... 60  
4.9. Summary ......................................................................................................................... 62  
5. The legal risks faced by young people using SNS ................................................................. 64
5.1. Terms of Service ............................................................................................................. 64
   ToS presented on a ‘take it or leave it’ basis ................................................................. 65
   Complexity of drafting and language ...................................................................... 65
   Age limitations ............................................................................................................... 66
   Applicable law ............................................................................................................... 66
   Disclaimer of liability ..................................................................................................... 66
   Monitoring and removal of content ........................................................................... 67
   Protection of user name and password ......................................................................... 67
   Acceptable user names ................................................................................................. 68
   Prohibited conduct ........................................................................................................ 68
   Intellectual property rights (IPRs) ............................................................................... 69
   Privacy policies ............................................................................................................. 70
   Summary ....................................................................................................................... 70
5.2. Legal risks of using SNS ............................................................................................ 71
   Privacy ......................................................................................................................... 71
   Copyright ...................................................................................................................... 73
   Defamation ................................................................................................................... 74
   Criminal laws: identity theft, harassment & offensive publications ......................... 76
5.3. Capacity and liability of minors ................................................................................ 78
   Legal capacity ............................................................................................................... 78
   Criminal liability ......................................................................................................... 78
5.4. A Modern Parable: Posting Photographs of Naked Footballers ................................. 78
5.5. Conclusion .................................................................................................................. 81
6. Regulatory & Policy Responses .................................................................................... 82
   6.1. Objectives of Regulating SNS ............................................................................... 82
   6.2. US Initiatives ........................................................................................................... 84
   6.3. European regulatory initiatives .............................................................................. 89
   6.4. Australian initiatives ............................................................................................. 93
      Commonwealth .......................................................................................................... 95
      New South Wales ....................................................................................................... 96
      Victoria ....................................................................................................................... 96
      Queensland ............................................................................................................... 96
      South Australia ......................................................................................................... 97
      Western Australia ..................................................................................................... 97
      Tasmania .................................................................................................................... 97
      Australian Capital Territory ....................................................................................... 97
      Codes of Conduct ...................................................................................................... 98
6.5. Summary .................................................................................................................... 99
7. Conclusion ...................................................................................................................... 100
   7.1. Research findings ................................................................................................. 100
   7.2. Recommendations ............................................................................................... 103
8. Bibliography .................................................................................................................. 106
# List of Tables

Table 1  Survey and Interview participants .......................................................... 20  
Table 2  Student participants' gender and year level ............................................ 21  
Table 3  Distribution of parent survey participants by location and year level ......... 21  
Table 4  Student participants: use of SNS, year level, system and location .......... 24  
Table 5  Teacher and parent knowledge of student/child using a SNS ................. 25  
Table 6  Use of SNS by student year and gender .............................................. 25  
Table 7  The most popular SNS used by students .............................................. 26  
Table 8  The most popular SNS used by students by year level ............................ 27  
Table 9  Frequency of students updating their own SNS by year level ................. 28  
Table 10 Frequency of students updating their own SNS by year level and gender .... 30  
Table 11 The activities for which students use SNS ........................................ 31  
Table 12 The activities for which students by year level use SNS ....................... 32  
Table 13 The activities for which students by year level use SNS by gender .......... 33  
Table 14 Methods of student communication with friends using SNS by year level .... 36  
Table 15 Methods of student communication using SNS by year level and gender ... 37  
Table 16 Types of SNS content posted by students by year level ........................ 38  
Table 17 Types of SNS content posted by students by year level and gender .......... 39  
Table 18 Do SNS profiles accurately reflect student identity (year) ...................... 41  
Table 19 Do SNS profiles accurately reflect student identity (year and gender) ....... 42  
Table 20 Types of SNS content posted by students’ friends ............................... 43  
Table 21 Are students concerned when their images are posted on friends’ SNS? .... 44  
Table 22 The importance of SNS to students ................................................ 44  
Table 23 The most valued aspect of SNS as reported by students ....................... 45  
Table 24 Perceptions of SNS degree of risk by students, teachers and parents ....... 47  
Table 25 Perceptions of degree of SNS risk by student year level ....................... 48  
Table 26 Perceptions of degree of SNS risk by student year level and gender ......... 49  
Table 27 Reported visibility of student SNS profiles ........................................ 50  
Table 28 Student perceived risks and problems associated with using SNS ......... 51  
Table 29 The extent of students talking with parents and teachers about SNS ....... 54  
Table 30 Teachers’ reports of discussing SNS risks with students ....................... 56  
Table 31 Parents’ reports of discussing SNS risks with their child ....................... 57  
Table 32 Strategies in response to unwelcome contact via SNS .......................... 58  
Table 33 Students’ reported strategies for avoiding SNS risks or problems ......... 58  
Table 34 Visibility of teachers’ SNS profiles ................................................ 60  
Table 35 Safer Social Networking Principles .................................................. 89  
Table 36 Evaluation of Implementation of Safer Social Networking Principles ...... 90
List of Figures

Figure 1. The most popular SNS used by students by year level .................................................. 27
Figure 2. Frequency of updating information on SNS across year levels (1) ................................. 29
Figure 3. Frequency of updating information on SNS across year levels (2) ............................... 29
Figure 4. Average frequency of male and female students updating their own SNS .................. 30
Figure 5. Student uses of SNS .................................................................................................. 32
Figure 6. The activities for which students by year level use SNS ............................................ 33
Figure 7. The activities for which students by year level use SNS by gender ............................ 34
Figure 8. Frequency of parents communicating with their child via SNS ................................. 35
Figure 10. Comparison of male and female students' use of SNS communication tools ............ 37
Figure 11. Types of SNS content posted by students ................................................................. 38
Figure 12. Year 7 types of content posted to their SNS ............................................................. 39
Figure 13. Year 8 types of content posted to their SNS ............................................................. 39
Figure 14. Year 9 types of content posted to their SNS ............................................................. 40
Figure 15. Year 10 types of content posted to their SNS .......................................................... 40
Figure 16. Do SNS profiles accurately reflect student identity (year) ........................................ 41
Figure 17. Do SNS profiles accurately reflect student identity (year and gender) .................... 43
Figure 18. The importance of SNS to students .......................................................................... 45
Figure 19. Perceptions of SNS risk by students, teachers and parents ........................................ 47
Figure 20. Perceptions of SNS risk by student year level ........................................................ 48
Figure 21. Comparison of male and female perceptions of degree of SNS risk ........................... 49
Figure 22. Visibility of student SNS profiles ............................................................................ 50
Figure 23. Risks or problems associated with SNS identified by year 7 to 10 students ............ 52
Acknowledgements

This publication has been supported with a General Grant from the Victoria Law Foundation. Website: www.victorialawfoundation.org.au. This is the report of Project G09-010 – Guidance for children engaged in social networking on the internet.

In addition, this research gratefully acknowledges the time and energy donated to this project by the 17 participating schools and their communities. In addition we acknowledge the invaluable insights of several experts from a number of fields including social media, cybersafety and teaching: Professor Jock Given, Robyn Treyvaud, and Melanie Saba.
Authors

Melissa de Zwart is an Associate Professor in the Adelaide Law School, The University of Adelaide. Her research interests are social networking, virtual worlds, copyright, the governance of online communities and the intersection between law and new communication technologies.

Email correspondence: melissa.dezwart@adelaide.edu.au

David Lindsay is an Associate Professor in the Faculty of Law, Monash University, Melbourne. He is the author of International Domain Name Law (2007), and an expert in internet law, copyright and privacy law. His current research focuses on social networking sites, ISP liability and copyright policy.

Email correspondence: david.lindsay@monash.edu

Michael Henderson is a Senior Lecturer in ICT in Education, in the Faculty of Education, Monash University, Melbourne. In addition to the affordances and risks of social networking in education, his research and teaching interests lie in teachers’ professional development, new learning technologies and online teaching and learning. Michael has won several teaching awards and regularly presents keynotes to teaching associations on engaging students through digital technologies.

Email correspondence: michael.henderson@monash.edu

Michael Phillips is a postgraduate research student in the Faculty of Education, Monash University, Melbourne. In addition to developing and implementing pedagogical approaches to using Web 2.0 technologies, his research focuses on the role of teacher identity and the transformations of identity along with teachers' planning and use of technologies across the curriculum.

Email correspondence: michael.phillips@monash.edu
1. Executive Summary

This project was established specifically to address an identified gap in the extant research by investigating the legal risks of social networking as experienced by Victorian secondary school students, teachers and parents. While risks posed by forms of abusive behaviour such as cyber-bullying and grooming have been emphasised, both in the mainstream media and in policy responses, comparatively little attention has been given to the potential legal risks that children and young people may face when they use social networking services (SNS).

This study surveyed 1004 middle school students (years 7-10), 204 middle school teachers and 49 parents of middle school students. In addition focus group interviews were conducted with 58 middle school students and 21 middle school teachers. The data was collected from 17 Victorian secondary schools from state (government run), Catholic and independent systems as well as metropolitan and rural locations.

In addition to collecting this empirical data, the authors conducted a comprehensive review of the literature, SNS Terms of Service (ToS), and the Australian and International regulatory environment.

The project identified the following as the main areas of the law that give rise to possible legal liability for young people using SNS:

- Privacy, disclosure and breach of confidence;
- Intellectual property rights, especially copyright infringement;
- Defamation; and
- Criminal laws, including harassment and offensive material.

The project found that young people, their parents, and teachers were generally aware that the use of SNS can give rise to risks that must be managed, however there was a worrying lack of understanding of the nature of the legal risks.

While, strictly speaking, minors may not be held legally liable for breaching the Terms of Service (ToS) of SNS, the worrying level of young users’ understanding of the obligations they have agreed to has implications for how they may understand their obligations in the future, as the ToS are likely to be binding on adults.

1.1. Key findings

The findings confirm that SNS usage has become integrated into the everyday social lives of most Victorian middle school students. The findings also indicate that there is a general awareness of risks in using SNS by middle school students, although concerns about risks differ markedly between parents and teachers, on the one hand, and students, on the other. However, there is very little clear understanding by students, parents and teachers alike, of the precise nature of the legal risks that may arise from everyday SNS use.

Key or noteworthy findings are listed here. An extended list can be found in Chapter 7.

1. The overwhelming majority (94.9%) of middle school students (years 7 to 10) have used SNS.
2. Facebook is the most popular SNS, with 93.4% of students using it, followed by MySpace, with 26.6% of surveyed students using it. Many students use more than one SNS.

3. The majority of surveyed students update information on their SNS at least every day, and over a quarter update their SNS profile several times a day.

4. The surveyed students use SNS primarily to maintain current social networks, while making new friends and flirting were relatively low in students’ reported practices.

5. The majority of parents (80.4%) indicated that they had seen their child’s SNS profile at least once.

6. The most common content reported as posted to SNS by surveyed students is photographs of themselves (60.9%), closely followed by photographs of their friends (52.6%). Nevertheless, posting of third party content, including music, video and photos of celebrities, is still significant. The proportion of students posting videos to SNS increases with age.

7. A significant proportion of students (45.6%) reported that their photos had been posted on their friends’ SNS. The majority of students were not concerned with this practice.

8. The most highly valued feature of SNS was the ability to stay in touch with friends and family. SNS are also perceived to be less expensive than other forms of communication.

9. Surveyed students felt that SNS were safer than did their teachers and parents. Thus, while 48.8% of students recognised that there was some element of risk in using SNS, more than one quarter (28.3%) thought that SNS were safe. Moreover, 19.6% of students were ambivalent about risk, essentially reporting that the degree of risk was irrelevant to them as it is “just what everyone does”.

10. Students from years 7 to 10 are increasingly more selective in who can see their profile. The survey results suggest that year 7 students not only have more visible profiles, but are more likely to perceive SNS as safe or only a little bit risky.

11. A majority of surveyed students (72.4%) indicated that they had had unwanted or unpleasant contact by strangers via their social networking profile.

12. A minority of students (13.8%) were concerned about security risks, such as identity theft. A small group of student respondents (3.2%) identified concerns relating to privacy or unwelcome disclosure of data.

13. Parents and teachers were particularly concerned with issues of cyber-bullying, and grooming or stalking, with a lesser number expressing concerns about identity theft and disclosure.

14. Despite the acknowledged risks of students using SNS, there is surprisingly little ongoing conversation about SNS use between parents and their children, on the one hand, or teachers and their students, on the other. In this respect, almost half of the surveyed students (46.1%) reported that they did not talk with their parents about SNS use, while almost three quarters of the students (74.6%) reported that they did not talk with their teachers about SNS use.

15. Surveyed students reported an awareness of a variety of strategies for avoiding risks or problems associated with SNS use, including ignoring ‘friendship’ requests from strangers, blocking or deleting unpleasant or unwanted friends, setting their
profile to ‘private’, not disclosing personal details, frequently changing their password, threatening people who wished to be added to the student’s SNS and self-censorship. Only 1% of respondents reported asking for guidance or help from adults as a viable strategy.

16. The majority of teachers have not used SNS in an educational context. However, a significant minority (36.1%) of the teachers who were asked this question indicated that they had used SNS for educational purposes, including communicating with their students about schoolwork.

17. The majority of teachers who were surveyed on the issue indicated that they were generally aware of risks, including legal risks, of teachers using SNS. However it is also clear that teachers had a variety of understandings about the specific nature of this risk.

1.2. **Key recommendations**

The key recommendations arising from this project are as follows:

1. **In order to enhance the benefits of SNS use, and minimise the disadvantages, it is important for children and young people to be equipped with the necessary information to empower them to effectively manage risks associated with the everyday use of SNS. The best way to do this is through specifically tailored educational activities. As children and young people must be primarily responsible for managing their own risks, it is essential that educational activities focus on providing clear and accurate information about all risks associated with SNS use, including legal risks. These educational activities should be aimed primarily at equipping children and young people with the skills required to be effective digital citizens, and not focussed on rare or hypothetical fears.**

2. **Education about the full range of legal risks potentially encountered by the use of SNS should be part of a fully integrated cybersafety school curricula. This means that attention that is properly given to more dramatic issues, such as cyber-bullying and ‘sexting’, should be balanced with attention to other potential areas of legal liability. This strategy should also assist in promoting awareness of, and debates about, the Australian legal system as it applies to online activities. While acknowledging the crowded nature of school curricula, the importance of SNS in the lives of students, and the potential significance of social media for future digital citizenship, suggests that room should be found for these issues to be directly addressed.**

3. **The best way to approach the teaching of legal literacy in the digital environment is by the use of practical examples drawn from real life case studies. With this objective in view, one of the outcomes of this project is the Education Resource Book, which includes a series of classroom exercises aimed at promoting understanding and discussion of specific legal issues. The researchers for this project encourage the production and use of this and similar resource material for the use of teachers of middle school students.**

4. **The reported prevalence of posting of photographs of students to SNS, suggests that the legal and ethical issues involved with the posting of photographs – which include privacy, confidentiality, defamation and copyright – merit specific attention in any cybersafety curriculum. The significance of understanding these**
issues is emphasised by the incidents involving a Melbourne teenager posting naked photos of AFL footballers to her Facebook site.

5. The potential disparities in the approaches to, and understandings of, legal risks associated with SNS use between parents, teachers and students, as well as the reported paucity of communication using SNS between students and parents and teachers, suggests that there is some need for education and training of teachers and parents, as well as students. Much can be gained by the community from greater informed discussion of the implications of SNS use, including legal implications, among parents, teachers and students.

6. Consideration should be given by Commonwealth, State and Territory authorities to encouraging SNS service providers operating in Australia to enter into a self-regulatory agreement similar to the Safer Social Networking Principles for the EU. This would provide baseline commitments against which practices of SNS service providers in their dealings with young people could be periodically assessed.

7. Given the concerns expressed by teachers interviewed for this project, there appears to be an identified need for further guidance to be provided to teachers about the use of SNS, especially in the pedagogical context. In particular, there is a pressing need for research and policy work to be undertaken in determining the extent of the ‘duty of care’ owed by teachers in any interactions with students via SNS. In this respect, it is important that the salient differences between interactions via SNS, and interactions offline, including the different legal implications, are fully taken into account.

8. There is a need to promote holistic policy responses to the full range of risks associated with the use of SNS by young people. Any responses should be coordinated so as to minimize the risk of fragmented, inconsistent, and potentially contradictory, policy initiatives at the Commonwealth, State and Territory levels. If, following the forthcoming report by the Commonwealth Joint Select Committee on Cyber-Safety, it is decided to establish an Online Ombudsman, the Ombudsman’s portfolio should extend to promoting education about the full range of legal risks associated with the use of SNS. In doing so, the Ombudsman should coordinate with Commonwealth, State and Territory Privacy Commissioners.

1.3. Publications

The two main research outcomes of this project have been:


In addition, a web-site has been established as a result of this project to provide resource for Victorian middle school students. The website can be accessed at: http://cemmx.educ.monash.edu.au/SNSrisks

The project has also resulted in a number of publications in peer-reviewed academic journals and conference proceedings. To date, the publications have consisted of the following articles and papers, which outlined the preliminary outcomes of the project:

[4]


The paper prepared for the Australian Council for Computers in Education Conference 2010 received a Highly Commended Paper Award. All of the publications acknowledged the support of the Victorian Law Foundation.

1.4. **Structure of the Report**

This report consists of the following sections.

2. **Introduction** - An explanation of the background to the project; the scope of the project, including explanations of SNS, the benefits and risks of using SNS, and the legal risks facing children and young people using SNS;

3. **Research design: Students SNS practices and perceptions of legal risk** - An explanation of the methodological issues relating to conducting surveys and interviews with students, parents, and teachers. This chapter also outlines the demographics of the research participants.

4. **Results: Students SNS practices and perceptions of legal risk** - An explanation of the empirical findings arising from the surveys and interviews with particular focus on the current practices of students in using SNS, and their perceptions of risks in using SNS.

5. **The Legal Risks Faced by Young People using SNS** - A description and analysis of the legal risks facing children and young people in the use of SNS, including explanations of the Terms of Service (ToS) governing the use of SNS; of the main areas of legal risk facing children and young people; and the capacity and liability of children and young people.

6. **Regulatory and Policy Responses** - Explanation and analysis of the main regulatory responses to legal risks to children arising from SNS, including initiatives that have been taken to date in the United States; in the European Union, including the UK; and in Australia, including Commonwealth, State and Territory initiatives.

7. **Conclusion** - This chapter provides a summary of the research findings and proposes a series of recommendations made by this project.
2. Introduction

2.1. Project background

Social networking sites (SNS) have rapidly become a ubiquitous method of communicating and socialising for Australian children and young adults. For example, a recent Australian Communications and Media Authority (ACMA) Report, *Click and connect: Young Australians’ use of online social media*, found that: ‘The internet is a regular part of everyday lives of children and young people aged eight to 17 years, and is used regularly both within school and home environments.’¹ From the age of 12 years, it appears that young people shift from using the internet primarily as a source of entertainment, predominantly for the playing of games, to using it as a means of socializing and communicating. As the ACMA report put it:

> 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.²

SNS, including MySpace and Facebook, offer new and varied ways to communicate and network via the internet, through either a personal computer or, increasingly, mobile phones. They provide a forum for users to create an online profile and to construct and display an online network of contacts (commonly known as ‘friends’), as well as to display media content which demonstrates their likes, dislikes and preferences.

Accordingly, interactions via SNS, are playing an increasingly important role in the lives of children and young people. In fact, they have arguably become an essential part of the life of a typical Australian teenager, to the point that opting out of participation in social networking is now inconceivable to those involved. The use of SNS has rapidly become so integrated within the fabric of everyday life for so many young people that it is, for many, if not for most, a crucial part of socialisation and identity formation.

The rapid growth in the use of SNS by young people has been accompanied by a range of policy initiatives, which commonly respond to community concerns relating to the risks these technologies may pose to vulnerable users. Thus, in Australia, policy responses to the use of SNS by young people are almost invariably characterised as part of programs aimed at promoting ‘cybersafety’. For example, the ACMA has an educational program that groups cybersafety issues under the following four general categories:

1. personal and peer safety, including privacy and inappropriate contact;
2. online behaviours, such as cyber-bullying and netiquette;
3. digital media literacy, including an understanding of computer technology, an awareness of the internet services that children use, tools available for parents, etc;
4. e-security, the technical tools to make a computer child safe including computer security, filters, viruses and malware.³

---

¹ Australian Communications and Media Authority (ACMA), 2009. *Click and connect: Young Australians’ use of online social media* (Canberra, July 2009) 5.


³ See Australian Communications and Media Authority (ACMA), 2010. *Cybersmart parents: Connecting parents to cybersafety resources* (Canberra, July 2010) 2.
The fears associated with the risks of online activities to children and young people, and especially the risks of cyber-bullying and predatory behaviour such as online grooming, are also reflected in the terms of reference for the Commonwealth Joint Select Committee on Cyber-Safety, which was established in September 2010, but has yet to report. In particular, the Committee’s terms of reference include inquiring into, and reporting on:

- the nature, prevalence, implications of and level of risk associated with cyber-safety threats, such as:
  - abuse of children online (cyber-bullying, cyber-stalking and sexual grooming);
  - exposure to illegal and inappropriate content;
  - inappropriate social and health behaviours in an online environment (e.g. technology addiction, online promotion of anorexia, drug usage, underage drinking and smoking);
  - identity theft; and
  - breaches of privacy.

While risks posed by forms of abusive behaviour such as cyber-bullying and grooming have been emphasised, both in the mainstream media and in policy responses, comparatively little attention has been given to the potential legal risks that children and young people may face when they use SNS. Yet the very real legal hazards facing teenage users of SNS were illustrated by a highly publicised event in late 2010, which involved the posting of photographs of naked St Kilda football players by a Melbourne teenager to her Facebook site. This project was established specifically to address an identified gap in the extant research by investigating the legal risks of social networking as experienced by Victorian secondary school students, teachers and parents, such as threats to privacy, potential infringements of intellectual property rights (IPRs), defamation, and other associated risks.

2.2. **Scope of the project**

*What is a social networking site (SNS)?*

The most commonly accepted definition of SNS, first proposed by boyd and Ellison, defines social network sites to mean ‘web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system’. As the authors explain, they deliberately avoided the use of the term ‘social networking sites’ (emphasis added) as:

> “Networking” emphasizes relationship initiation, often between strangers. While networking is possible on these sites, it is not the primary practice on many of them,

nor is it what differentiates them from other forms of computer-mediated communication (CMC).\(^7\)

As Grimmelman has explained, the three elements of the boyd and Ellison definition can be interpreted as corresponding to three aspects of social interaction via SNS:

The first prong – profiles - emphasizes identity: users create profiles that represent them. The second prong – contacts - emphasizes relationships: users establish one-to-one connections with others. The third prong - traversing lists of contacts - emphasizes community: users occupy a specific place among their peers.\(^8\)

The definition has not, however, been immune from criticism. For example, Beer has argued that it is precisely the fact that ‘networking’ is the main preoccupation that sets apart SNS, properly speaking, from sites, such as YouTube, involving other collaborative activities.\(^9\)

Within the context of policies aimed at protecting children and young people, the European Union (EU) has developed the *Safer Social Networking Principles*, which adopted a more comprehensive definition of SNS as online services that combine the following features:

- A platform that promotes online social interaction between two or more persons for the purposes of friendship, meeting other persons, or information exchange;
- Functionality that lets users create personal profile pages that contain information of their own choosing, such as the name or nickname of the user, photographs placed on the personal page by the user, other personal information about the user, and links to other personal pages on the service of friends or associates of the user that may be accessed by other users or visitors to the service;
- Mechanisms to communicate with other users, such as a message board, electronic mail, or instant messenger; and
- Tools that allow users to search for other users according to the profile information they choose to make available to other users.\(^10\)

The debate about how central networking activities are to the definition of SNS is, to some extent artificial, as there is some degree of networking even on sites that are directed more to other activities, such as content sharing. Moreover, research undertaken for this project indicated that young people often link material from sites that are not, strictly speaking, SNS, such as YouTube, to their SNS profile. As this research project was directed at investigating the legal risks facing children and young people, it has adopted the wider definition of SNS proposed by boyd and Ellison, which allowed us to capture as broad a range of relevant student activities as possible.

Applying this broad definition, the project survey identified the following SNS as especially relevant to Victorian High School students:

- *Bebo* – whose name is an acronym of ‘blog early, blog often’, is an SNS launched in July 2005, which is owned by Criterion Capital Partners. Bebo incorporates features of most SNS, including user profiles, a list of ‘friends’ and the ability to link to YouTube.

- *Tumblr* – a microblogging platform, that permits users to post text, photos, quotes, links, chat, audio and video.

\(^7\) Ibid.


• **Twitter** – is mostly known as a web-site that provides a microblogging service, allowing users to make short, text-based posts of up to 140 characters, known as ‘tweets’, that are visible on the user’s profile page.

• **MySpace** – a well-known SNS, that includes user profiles, and the ability to post a wide range of content. Until it was overtaken by Facebook in April 2008, Myspace was the most popular SNS. In late 2010, largely in response to the dominance of Facebook, Myspace was re-designed to focus more on music and young people.

• **Facebook** – is the most popular SNS, which allows users to create and update profiles, add ‘friends’, upload photos and use a ‘chat’ facility.

### 2.3. Benefits and risks of SNS

The response of the mainstream media and policy-makers to the rapid uptake in the use of SNS by children and young people has, like much commentary on the use of media by young people, focussed mainly on the risks posed by the technology. For example, there have been many instances, reported by the media, of SNS being used to bully, mislead and even form suicide pacts. One prominent example was the media’s use of photographs of Australian Olympic swimmer Stephanie Rice at a private party, which was used as a warning of the unforeseen risks of setting privacy settings of a SNS to allow public viewing.\(^\text{11}\) Considerable recent attention has also been given to the practice of children placing naked and explicit photos of themselves and their friends, or photos sent to them via mobile phones (termed ‘sexting’), on sites such as Flickr.\(^\text{12}\) These high-profile examples highlight the extent to which the repercussions of engagement with social networking can be both far-reaching and commonly unforeseen by the individual involved.

While it is important to acknowledge the risks that may arise from young peoples’ use of SNS, most experts have been concerned to point out that the potentially significant benefits that may arise from the use of networking technologies should not be overlooked. For example, in 2008, Professor Tanya Byron, a clinical psychologist, conducted an independent review of child online safety for the UK government.\(^\text{13}\) While acknowledging that there are real risks involved with children’s use of online and digital media, the *Byron Review* found that over-emphasis on online risks played into a broader ‘risk-averse’ culture, which had the potential to hinder rather than promote child development. Endorsing the view emerging from the research that a certain amount of risk taking is essential for the healthy development of children and young people, the Review proposed an approach based on empowering children to manage risks rather than protecting them from all risks. In other words, it advocated moving:

> … from a discussion about the media ‘causing’ harm to one which focuses on children and young people, what they bring to technology and how we can use our understanding of how they develop to empower them to manage risks and make the digital world safer.\(^\text{14}\)

As Dr Karen Vered put it, in rejecting an approach based on eliminating all risks, in her submission to the Joint Select Committee on Cyber-Safety:

---

12 See, for example, Carey, A. 2010. ‘‘Sexting’ teens breach child porn law’, The Age, 10 December 2010, 3.
14 Ibid. 2.
Children will not learn from mistakes if filtering and blocking software prevent them from ever having to exercise judgment. If we place children inside a walled garden, we deny them the opportunity to practice the self-management and self-regulation skills that we want them to have.\textsuperscript{15}

Similarly, a 2007 ACMA report on media and communications in Australian families reported that:

The academic literature on internet use indicates that despite concerns and potential risks, children and young people use the internet for communication and the management of interpersonal relations, identity building, creative activities, and for learning.\textsuperscript{16}

A 2008 report produced for the US MacArthur Foundation digital media and learning initiative was more specific about the potential benefits for young people in using new social media, including:

- \textit{Social and recreational new media use as a site of learning} – it is important to appreciate that young people who are interacting socially online are accumulating social and technological skills that are needed to participate in contemporary society.

- \textit{Diversity in forms of media literacy} – online interactions range from purely friendship-driven to interest-driven, but each may have benefits in terms of socialising or education that are necessary for participation in future social or work environments.

- \textit{Peer-based learning} – use of new media facilitates learning from peers, which has some advantages over learning from adults, including teachers.

- \textit{Changing role of education} – the participation of young people in social media presents important new learning opportunities, if educational practices can harness the power of the new social tools.\textsuperscript{17}

A relatively recent comprehensive statement of the key benefits and the potential risks facing young people in the use of new social media was compiled by the US Federal Communications Commission (FCC) in a 2009 notice soliciting submissions for an inquiry into empowering parents and protecting children in an evolving media landscape. The most important benefits identified by the FCC were:

- Access to educational content;
- Acquiring technological literacy needed to compete in a global economy;
- Developing new skills in the use of technology and the creation of content;
- Facilitating new forms of communication with family and peers; and
- Removing barriers for children with disabilities.\textsuperscript{18}

\textsuperscript{15} Dr Karen Vered, Submission to Joint Select Committee on Cyber-Safety, Submission No. 68, 23 June 2010, 3.
On the other hand, the FCC identified the following risks associated with the use of new social media, which include both novel risks, and new forms of old risks:

- Exposure to inappropriate content (including offensive language, sexual content, violence, or hate speech);
- Potential impact on behaviour;
- Harassment and bullying;
- Sexual predation;
- Fraud and scams;
- Failure to distinguish between who can and who cannot be trusted when sharing information;
- Compromised privacy; and
- Exposure to exploitative advertising, or use of user information, by SNS providers.\(^\text{19}\)

Some teachers and educational researchers have given more specific attention to the potential educational advantages of SNS use. For instance, Dalsgaard has argued that ‘social networks support self-governed, problem-based and collaborative learning processes’, and consequently lend themselves to student-centred learning.\(^\text{20}\) A review of the educational research reveals considerable support for the use of what is known as ‘social software’ tools, such as Web 2.0 tools and SNS, in the design of educational curricula.

The question of the use of SNS as an educational tool clearly illustrates some of the practical difficulties in balancing the benefits and risks of SNS. As SNS are essentially a platform for online social networks, they allow for interactions outside of the traditional physical and social context of the school. In this respect, educational authorities have naturally expressed concerns about the appropriateness of teachers ‘friending’ students, including the potential risks facing both teachers and students of exposure to inappropriate conduct or content. Indeed, as explained later in this report, in some Australian states education authorities have banned teachers from using SNS to contact students.

2.4. What are the legal risks?

Just as attention has focussed on high-profile risks associated with the rise in use of SNS by young people, such as cyber-bullying, online grooming and sexting, consideration of specific legal risks has tended to focus mainly on potentially abusive interactions. For example, the Australian government has established a Consultative Working Group on Cybersafety (CWG), which consists of representatives from industry, community organizations and Commonwealth government agencies, and whose role is to consider all aspects of cybersafety faced by Australian children. The CWG has indicated that the main focus of its work is on:

- Cyber-bullying;

\(^\text{19}\) Ib. Id. 3.
• Inappropriate handling of one’s own and others’ private information;
• Exposure to and creation of inappropriate content;
• Computer gaming addictions; and
• Sexual predation.  

While the more dramatic threats to children have received widespread publicity, much less attention has been given to the extent to which everyday use of SNS can give rise to a range of risks of legal liability which do not exist, or which exist to a lesser degree, in the offline world. In particular, online social interactions differ from offline social interactions in potentially legally significant respects, including: that they are more visible; they may be published to a potentially wider audience than an offline social group; and they may leave a relatively permanent record, with the consequent potential to affect users for some time into the future. In other words, the migration of social interactions to SNS has important legal implications, as well as social and psychological implications. Moreover, empowering children and young people to manage their own risks, and to be effective digital citizens, necessarily involves education relating to the consequences of online activities and conduct, which should include the potential legal consequences of everyday online behaviour.

The research undertaken for this project therefore did not focus on cyber-bullying, online predation or sexting, which have already received considerable attention, but on the relatively less dramatic, but no less important, legal risks which may accompany common uses of SNS. The project identified the following as the main areas of the law that give rise to possible legal liability for young people using SNS:

• Privacy, disclosure and breach of confidence;
• Intellectual property rights, including copyright and trade mark protection;
• Defamation; and
• Criminal laws, including harassment and offensive material.

Each of these areas of potential liability merits further explanation. In addition to the above areas the project considered that it was important to examine the extent to which young users are aware of their obligations under the contractual Terms of Service (ToS) that are agreed to when users join a SNS.

**Privacy, Disclosure and Confidentiality**

The popularity of SNS among school students gives rise to two distinct kinds of threats to privacy. The first set of concerns relates to the disclosure of personal information by the students themselves. Applying the principle of user autonomy, this does not give rise to risks of legal liability, but may give rise to a range of risks, including misuse of the information by other people. The second set of concerns, on the other hand, relates to the posting of personal information about a student by other people, including the possibility of other people altering someone’s personal information.

SNS are built on the ‘sharing’ of information, including users posting their own text, photographs and video images. In a sense, then, they are built on users exposing aspects of themselves to others online. But in the online environment the consequences of posting

personal information are not always immediately apparent. There is evidence to suggest that, for a variety of reasons, young people may be less cautious about posting private information to SNS than are older users. For example, the July 2009 ACMA study, *Click and connect*, found that:

> 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. ... 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).

Similarly, a Community Attitudes Survey conducted by the Commonwealth Office of the Privacy Commissioner in 2007 found that respondents aged 18 to 24 years were less aware of their privacy rights than older respondents, suggesting that this may correspond with lower levels of awareness of legal rights more generally among young people.

Poorly thought-through disclosure of personal information, such as information about sexual activities, alcohol use or drug taking, may have immediate negative consequences. For example, disclosure of personal information can lead to consequences such as stalking, identity theft, harassment, or even blackmail. Sometimes, however, the consequences are not so immediately apparent. Nevertheless, the discovery of personal information by people for whom it was not intended, such as future employers or university officials, may have long-term negative consequences.

Although young people may now seem more willing to share personal information than previous generations, this is not necessarily indicative of a lack of concern about privacy, or a complete lack of attention to the management of personal information. Thus, a 2007 study of the use of SNS by American teenagers by the Pew Internet & American Life Project reported that:

> Most teenagers are taking steps to protect themselves from the most obvious areas of risk ... Most teens believe some information seems acceptable – even desirable – to share, while other information needs to be protected.

If young people retain concerns about privacy what, then, motivates some of their apparently cavalier attitudes to the disclosure of personal information on SNS? In a 2009 study of 263 Sydney secondary school students, De Souza and Dick concluded that there were a number of key drivers that encourage young people to disclose personal information on SNS, including:

- *Peer pressure*. De Souza and Dick, as well as previous studies, highlight the very significant role of peer pressure in youth decision-making, which often leads to high levels of disclosure of personal information.

---

22 Australian Communications and Media Authority (ACMA). 2009. *Click and connect: Young Australians’ use of online social media* (Canberra, July 2009) 8.


26 See, for example, Govani, T., & Pashley, H. 2005. Student awareness of the privacy implications when using Facebook, from http://lorrie.cranor.org/couses/fa05/tubzhp.pdf
• **Signalling.** SNS are commonly used in the construction of online identity through signalling. The more the user desires to portray him/herself in a certain light, however, the more likely he/she is to disclose a variety of information to support the desired perception. As Donath and boyd have suggested, for young SNS users the benefit of presenting oneself in a positive light may outweigh the costs of possible privacy invasions.\(^{27}\)

• **Trust.** Users of SNS may disclose personal information as they may be overly trusting of the social network website, or other SNS members. Moreover, the disclosure of personal information by other SNS users may have a snowballing effect, encouraging greater levels of trust than may be warranted.

• **Myopic view of privacy.** Many young users may have a poorly-developed understanding of privacy, which may lead them to under-estimate the true costs of revealing personal information. As Lenhart and Madden have pointed out, not all teenagers are aware of the risks of posting information to a public and durable environment, such as an SNS.

• **SNS Design.** The design interface of SNS is clearly aimed at encouraging users to share information (including personal information) by, for example, providing for the creation of profiles and lists of ‘friends’. In addition, some privacy options, such as the public sharing of photos, may be set to allow public access by default. Moreover, technological mechanisms for ‘protecting’ privacy may be ineffective. For example, registration forms, privacy options and the proliferation of choices can be confusing or misleading, especially for young people, or may simply be difficult to navigate.

While the exposure of a student’s own personal information may give rise to non-legal risks, publishing personal information about others has the potential to create legal liability. As well as sharing one’s own personal information, SNS provide the ability for users to publish personal information about others, including text, photographs and videos. For example, a teenager may post naked images of friends, or of friends engaged in recreational drug taking. At the extreme, the posting of embarrassing or lewd information relating to others, whether true or not, merges into cyber-bullying.

The posting of private or embarrassing information about other people clearly raises the issue of how best to effectively protect young peoples’ privacy while preserving the ability of young people to freely interact online. This is obviously a difficult balance to achieve, but educating young users about the potential legal implications of posting private information about other people is clearly one element in doing so.

**Intellectual property, risk and social networking**

SNS are used to create and project the user’s identity, to strengthen existing social links and, in some cases, to forge new ones. These activities are conducted predominately through the vehicle of the user’s online ‘identity’ or ‘profile’. A common way of building an online profile is through the display of images or extracts from popular culture, which sends a particular message about the user. For instance, the use of a celebrity or cartoon character photo as one’s Facebook profile image sends important messages about one’s identity.

Although the user is not necessarily aware of it, much of the content used in the construction of identities on SNS is protected by intellectual property rights (IPRs), especially copyright. The general approach taken by young people to the use of this material was helpfully explained by Palfrey and Gasser in their 2008 book, *Digital Natives*:

---

These young people are not passive consumers of media that is broadcast to them, but rather active participants in the making of meaning in their culture. Their art form of the remix, where digital files are combined to create a new video or audio file, is already having an effect on cultural understanding around the world. Creativity is the upside of this brave new world of digital media. The downside is law-breaking. The vast majority of Digital Natives are currently breaking copyright laws on a regular basis.

The appropriation of popular culture by young people in this way raises important policy questions, including how best to educate young users about copyright law. Moreover, in assessing these issues, it needs to be borne in mind that the very way in which SNS are structured encourages users to upload content, regardless of who owns the content. For example, as Williams has observed:

The templates ask people to think of their identities in terms of popular culture references: with the requests for lists of favourite movies, television programs, books; with the capability to choose a song to play when the page opens; and with the capability to load images and video from other sources.

Often users, and especially young users, assume that because their use of content is not for profit, but for the purpose of social interactions, they do not require permission from copyright owners to use copyright-protected music or images on their SNS sites. As explained in chapter 4, however, this assumption is unfounded. Furthermore, if users post their own material – such as artwork, stories or photographs – to their SNS pages, even if the user is unaware of it, this material is likely protected by copyright. The dual roles of young people using SNS as both users and creators of copyright material raise a range of important issues with potentially significant legal implications, including:

- The importance of understanding relevant provisions in the ToS of the SNS. For example, as further explained in chapter 2, the ToS may prohibit posting of content that infringes IPRs. On the other hand, the ToS may confer rights on the SNS provider over the content posted by SNS users.

- In particular, the importance of understanding the effect of any copyright licences over material posted to a SNS incorporated in the ToS of the SNS. In this respect, it appears that many users do not read or understand the terms of standard form licences, including Creative Commons (CC) licences. For example, in September 2007, a family in Texas filed an action against Virgin Mobile Australia, Virgin Mobile USA and Creative Commons with respect to the use by Virgin Mobile Australia of an image of teenager Alison Chang, which had been downloaded from Flickr. The photo had been taken by a family friend and uploaded by another family member, who tagged it with the default CC share-alike licence. The image was then used in the Virgin ‘Dump Your Pen Friend’ advertising campaign. Virgin claimed that the use was permitted by the terms of the CC licence.

- The importance of understanding that merely because some activities are commonly practised, or appear to be condoned, it does not mean that these practices are lawful. For example, young people often use SNS to post and communicate material among communities of fans of popular culture phenomena, such as Harry Potter or Twilight. Some of this material, such as fan fiction, may involve considerable effort on the part of the user concerned. Yet it may well be that this activity amounts to a breach of copyright. For example, in a recent US case, JK Rowling and Warner Brothers successfully sued the publishers of a Harry Potter lexicon for copyright infringement.

- The complexity of copyright law, which means that it is sometimes difficult to give definite advice about whether a particular activity amounts to an infringement, can act
as a barrier to people, regardless of their age, developing a good understanding of their rights and obligations under copyright law. For example, as explained in chapter 2, copyright may be infringed by using a ‘substantial part’ of a copyright-protected work, such as a song, picture or photograph. As what amounts to a substantial part is determined mainly by reference to the qualitative significance of the part that is taken, there is often room for debate about whether or not there has been an infringement. While the legal and policy issues associated with the use of copyright on SNS are complex and controversial, the dual roles of young people as users and creators provide an important opportunity for engaging them in discussions about IPRs. Acknowledging this, Palfrey et al have outlined a Creative Rights Copyright Curriculum, which is intended to educate students regarding creation and re-use of copyright material. In any case, as students are increasingly using, creating and communicating copyright material by means of SNS, it is important for them to be given some copyright guidance to assist them with their decision-making.

Defamation

As a form of social interaction, the use of SNS invariably includes gossip about people, including material that may be insulting or offensive, or that is likely to be interpreted as such. While insulting or offensive comments may be a relatively common, if unwelcome, part of offline interactions, social interactions via SNS take place in a different context. The context of SNS interactions differs from offline socialising as the interactions may be accessible to a wider audience, and a relatively permanent record of the interactions may be kept.

Defamation is a social tort, which protects the social reputation of a person from untrue comments or innuendos. While rumour-mongering and gossip may be regarded as an accepted, if unpleasant, incident of offline social interactions, participating in online social media effectively transforms a person into a publisher. Moreover, unlike traditional publishers, like the press or broadcasters, the spontaneous nature of social media means that users are more likely to make unguarded, potentially defamatory comments. The consequences were illustrated in November 2010, when *The Australian*’s editor-in-chief, Chris Mitchell, threatened to sue academic, Julie Posetti, for defamation. Posetti had tweeted comments allegedly made at a conference by a former journalist at *The Australian*, which suggested that Mitchell instructed journalists about what to write on climate change.

While children and young people, as well as their parents, may regard the risk of being sued for defamation as relatively slight, or non-existent, just as it is important to build an understanding of how the exposure of personal information may have potentially serious consequences, so it is important to learn of the potentially serious consequences of publishing unguarded comments, or other potentially defamatory material, about another person.

Criminal laws: harassment and offensive material

Since the 1990s, a range of new criminal laws have been introduced to deal with online crimes which, collectively, are commonly referred to as cybercrimes. Some of these criminal laws have potential application to the use of SNS by young people. As a submission by the Australian Institute of Criminology to the cyber-safety committee inquiry put it:

Undeniably, ICT have created a new space in which children and young people can both learn and play. It is a place of both opportunity and risk where they can develop but where they may also become the victims of crime or engage in illegal behaviour themselves.
As explained further in chapter 4, this project has identified three sorts of cybercrimes that are particularly relevant to the use of SNS by children and young people: identity theft, criminal harassment and similar offences, and offences relating to the publication of offensive material.

First, in relation to identity theft, young users need to be aware of the risks associated with disclosing identifying information, and become familiar with strategies for managing such information. On the other hand, it is equally important to understand that assuming someone else’s identity – such as using an adult’s credit card for an unlawful purpose – may give rise to potential criminal liability.

Second, there are a number of offences that involve criminal misuse of the internet, including threatening to kill or cause serious harm to a person, or menacing or harassing a person. Our research indicated that teenagers are capable of posting some quite strong statements to SNS. Given the concerns reported by our respondents about potentially abusive interactions, including cyber-bullying, it is possible that this kind of behaviour could escalate to criminal menacing or harassment.

Third, cybercrimes include a range of offences relating to the use of, access to, and distribution of child abuse material and child pornography. As minors can be charged with offences for sending and receiving images of themselves, or others, that fall within these categories, it is that young people familiarise themselves with these laws.

While the use of SNS may create the impression that they are consequence-free zones, the categories of cybercrimes mentioned above clearly illustrate how this is not the case. An understanding of potential criminal liability is therefore an essential part of creating a broader appreciation of potential legal risks associated with SNS use.

2.5. Summary

Although media and regulator focus has been directed largely to cyber-bullying issues, as the discussion above illustrates, there is a much larger range of risks posed to and by teens using SNS. These include privacy, intellectual property infringement, defamation, and criminal offences. While teens may not be aware of, or may disregard these risks, a common aspect of teen behaviour, the consequences of activities which breach any of these laws may have serious and very long terms effects. The research project identified a need to examine whether Victorian teens were aware of these risks and what their attitudes and responses to these risks might be. It was also considered important to develop an understanding of the perceptions of and attitudes to such risks by the parents and teachers of these students, to fully appreciate the context within which the use of SNS was occurring. Risks could be misunderstood both in terms of over and understating the impact that they may have on users. For example, parents may be most concerned about 'stranger danger' and contact from unknown third parties, whereas privacy risks may more likely be caused by unwanted posting of photos and links from friends of friends. Thus the project addressed a gap in the existing studies of use of SNS by focussing on conduct other than cyber-bullying. It was therefore necessary to design and undertake a large scale survey, to canvass the range of attitudes across different schools in Victoria, covering public and private schools, and urban and regional locations.
3. Research Design:

Student SNS practices and perceptions of legal risk

This project utilised a mixed methods approach to identify the current social networking practices of Victorian students in years 7 – 10 (known as middle phase or middle school students), as well as the perceptions of risk, particularly legal risk, of those students, their teachers and parents.

Mixed methods research involves concurrent or sequential use of qualitative and quantitative research approaches to address a research topic. It is argued that the combination of quantitative and qualitative approaches provide a better understanding of research problems than if only one of those approaches was used. This is especially true of research relating to complex social phenomena such as education and especially that of children’s understanding, learning and motivations.

In this research a quantitative approach was used in the form of an anonymous survey to students, parents and teachers. The survey identified current SNS practices of students as well as provided comparative data on all three participant groups’ perceptions of risk and risk aversion strategies. The qualitative data was derived from open ended questions in the survey but primarily through focus group interviews of students and teachers. A staggered approach to the research inquiry meant that the student, teacher and parent surveys were administered in one school followed by focus group interviews with students and teachers. This staggered approach allowed the researchers to validate the reliability of the researchers’ interpretation of the survey data as well as pursue in the interviews any emerging themes from the surveys. This approach also allowed the researchers to add to surveys prior to being implemented in other schools based on unexpected themes arising from the interviews. This process of adding to the survey questions ensured that a core set of questions could be compared across the entire participant set while at the same time providing the researchers with the ability to pursue new lines of inquiry albeit with a smaller data set. An example of this can be seen in the addition of survey questions relating to teacher’s own use of SNS for education purposes and their perceived risks of their own use. This line of inquiry arose from reported concerns of teachers in the interviews and was reflected the increased interest in teachers’ use of SNS by the media and teacher regulatory bodies.

The project was implemented in seven stages:

<table>
<thead>
<tr>
<th>Stages of research design and implementation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 2 3 4 5 6 7</td>
<td>ongoing</td>
</tr>
</tbody>
</table>

**Literature review:**
A review of policy, research literature, and the regulatory environment of social networking sites in Australia and internationally with a particular focus on the United Kingdom and United States.

**Research ethics approval:**
Receipt of permission to conduct research from the Monash University Human Research Ethics Committee, the Department of Education and Early Childhood Development, and the Catholic Education Office.

**Survey of students, parents and teachers:**
Large scale anonymous surveys of Victorian middle school students, teachers and parents in state, Catholic and independent sectors, as well as in metropolitan and regional locations. The surveys were primarily aimed at identifying student SNS practices as well as perceptions of what represents risky behaviour within the context of social networking.

**Focus group interviews with students and teachers:**
Focus groups with students and teachers with the aim of qualifying the survey results with more detailed responses, as well as gaining a more complex understanding of students and teachers risk perceptions and practices. The interviews were conducted across educational sectors and in metropolitan and rural locations.

**Analysis of data - mapping the risks:**
Mapping the survey and interview data to the literature review and regulatory frameworks review to identify legal risks.

**Semi-structured interviews with experts:**
Semi-structured interviews were conducted with experts in related fields to the research focus. A key purpose of these interviews was to strengthen the reliability of the researchers’ analysis of survey and interview data as well as to probe for additional issues not highlighted by the research participants or literature review.

**Reporting of findings:**
The preparation of the research outcomes, including (a) an educational resource package with user-friendly information for free distribution to all Victorian schools, teachers, students, and parents and (b) this research report.

3.1. **The participants**

The participants were drawn from schools across state (government), Catholic and Independent sectors as well as from metropolitan and rural settings (see Table 1 for details on
the distribution). The researchers contacted the principals of 250 secondary schools in Victoria with an invitation for their school to participate in this research. The response was unsurprisingly slow due to both principals and teachers being time poor. After eight months of recruitment 17 schools had agreed to participate. While this number was smaller than hoped for it still resulted in a pleasing survey response rate for students (1004) and teachers (204) because multiple classes and even entire year levels in many schools participated.

Unfortunately, but again not surprisingly, the parent participant group had a low level of response (49) to the survey invitations. Parent participation in educational research is notoriously low, which does not necessarily reflect a lack of parental interest but rather is symptomatic of the complex process of inviting parents (invitations typically have to pass through the hands of the principal to the teacher and then to the students who have to not only take the invitations to their parent/guardian but also choose/remember to give the invitations to them). In addition to the surveys, focus group interviews were conducted with 58 middle school students and 21 middle school teachers.

Table 1
Survey and Interview participants

<table>
<thead>
<tr>
<th>System</th>
<th>Location</th>
<th>n</th>
<th>Surveys</th>
<th>Interviews</th>
<th>Surveys</th>
<th>Interviews</th>
<th>Surveys</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metropolitan</td>
<td>Melbourne</td>
<td>7</td>
<td>600</td>
<td>17</td>
<td>80</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(59.8%)</td>
<td>(29.3%)</td>
<td>(39.2%)</td>
<td>(14.3%)</td>
<td>(24.5%)</td>
</tr>
<tr>
<td>Rural Victoria</td>
<td></td>
<td>7</td>
<td>262</td>
<td>23</td>
<td>87</td>
<td>12</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(26.1%)</td>
<td>(39.7%)</td>
<td>(42.7%)</td>
<td>(57.1%)</td>
<td>(46%)</td>
</tr>
<tr>
<td>Catholic</td>
<td>Metropolitan</td>
<td>2</td>
<td>114</td>
<td>18</td>
<td>31</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Melbourne</td>
<td></td>
<td>(11.4%)</td>
<td>(31%)</td>
<td>(15.2%)</td>
<td>(28.6%)</td>
<td>-</td>
</tr>
<tr>
<td>Independent</td>
<td>Metropolitan</td>
<td>1</td>
<td>28</td>
<td>-</td>
<td>6</td>
<td>-</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Melbourne</td>
<td></td>
<td>(2.7%)</td>
<td></td>
<td>(2.9%)</td>
<td></td>
<td>(28.6%)</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>17</td>
<td>1004</td>
<td>58</td>
<td>204</td>
<td>21</td>
<td>49</td>
</tr>
</tbody>
</table>

The seven rural schools were between 40kms - 250kms from Melbourne. The exception to this was that a School in the vicinity of Berwick (45kms) was classed as an outlying suburb of Metropolitan Melbourne.

The reason for targeting middle school students (years 7-10, approximately aged 12 to 16) was because this group typically experiences a number conditions such as the beginning of adolescence, the increase in autonomy and reduction of adult supervision, an increase in the significance of peer group interaction, an increased ownership or access to internet enabled devices, the minimum age group of a number of SNS including Facebook, and a flexible curriculum which may provide opportunities to explore educational applications of SNS.

Table 2 identifies the distribution of student survey responses according to year level, sector, location and gender. Each of the four year levels (7-10) are well represented in the survey. There was a greater response from year 9 students and a smaller number of overall responses in the Catholic and independent schools. However, the researchers caution any attribution of significance in the response rates since student surveys were administered by teachers in school time and as such the responses were dependent on teacher access, opportunity and motivation rather than student interest.

Due to an error in the initial survey distribution no data was collected on student gender in 174 surveys (17.3%). The majority of those surveys (138) were from the rural state schools and accounted for 52.6% of all surveys in those schools. In addition, the Catholic and independent schools were single sex schools. As a result this report is cautious in making generalisations based on gender, especially in regard to rural, Catholic and independent schools. Nevertheless,
of those surveys which included data on gender, 452 (45% of the total surveys) indicated they were male and 378 (37.7% of the total surveys) indicated they were female.

Table 2
Student participants’ gender and year level

<table>
<thead>
<tr>
<th>Year level</th>
<th>n</th>
<th>Student gender</th>
<th>Metropolitan State</th>
<th>Metropolitan Catholic</th>
<th>Metropolitan Independent</th>
<th>Rural State</th>
<th>Total</th>
<th>n</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>219</td>
<td>Male</td>
<td>56</td>
<td>1</td>
<td>0</td>
<td>20</td>
<td>77</td>
<td>35.2%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Female</td>
<td>58</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>63</td>
<td>28.8%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No data</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>79</td>
<td>79</td>
<td>36.0%</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>215</td>
<td>Male</td>
<td>85</td>
<td>0</td>
<td>0</td>
<td>17</td>
<td>102</td>
<td>47.5%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Female</td>
<td>59</td>
<td>39</td>
<td>0</td>
<td>10</td>
<td>108</td>
<td>50.2%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No data</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>2.3%</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>357</td>
<td>Male</td>
<td>90</td>
<td>36</td>
<td>0</td>
<td>16</td>
<td>142</td>
<td>39.8%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Female</td>
<td>91</td>
<td>0</td>
<td>28</td>
<td>14</td>
<td>133</td>
<td>37.3%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No data</td>
<td>28</td>
<td>0</td>
<td>0</td>
<td>54</td>
<td>82</td>
<td>22.9%</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>213</td>
<td>Male</td>
<td>62</td>
<td>38</td>
<td>0</td>
<td>31</td>
<td>131</td>
<td>61.5%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Female</td>
<td>63</td>
<td>0</td>
<td>28</td>
<td>11</td>
<td>74</td>
<td>34.7%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No data</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>3.8%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>Metropolitan State</th>
<th>Metropolitan Catholic</th>
<th>Metropolitan Independent</th>
<th>Rural State</th>
<th>Total</th>
<th>n</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>219</td>
<td>Male</td>
<td>56</td>
<td>1</td>
<td>0</td>
<td>20</td>
<td>77</td>
<td>35.2%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Female</td>
<td>58</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>63</td>
<td>28.8%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No data</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>79</td>
<td>79</td>
<td>36.0%</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>215</td>
<td>Male</td>
<td>85</td>
<td>0</td>
<td>0</td>
<td>17</td>
<td>102</td>
<td>47.5%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Female</td>
<td>59</td>
<td>39</td>
<td>0</td>
<td>10</td>
<td>108</td>
<td>50.2%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No data</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>2.3%</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>357</td>
<td>Male</td>
<td>90</td>
<td>36</td>
<td>0</td>
<td>16</td>
<td>142</td>
<td>39.8%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Female</td>
<td>91</td>
<td>0</td>
<td>28</td>
<td>14</td>
<td>133</td>
<td>37.3%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No data</td>
<td>28</td>
<td>0</td>
<td>0</td>
<td>54</td>
<td>82</td>
<td>22.9%</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>213</td>
<td>Male</td>
<td>62</td>
<td>38</td>
<td>0</td>
<td>31</td>
<td>131</td>
<td>61.5%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Female</td>
<td>63</td>
<td>0</td>
<td>28</td>
<td>11</td>
<td>74</td>
<td>34.7%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No data</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>3.8%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>Metropolitan State</th>
<th>Metropolitan Catholic</th>
<th>Metropolitan Independent</th>
<th>Rural State</th>
<th>Total</th>
<th>n</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>219</td>
<td>Male</td>
<td>56</td>
<td>1</td>
<td>0</td>
<td>20</td>
<td>77</td>
<td>35.2%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Female</td>
<td>58</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>63</td>
<td>28.8%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No data</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>79</td>
<td>79</td>
<td>36.0%</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>215</td>
<td>Male</td>
<td>85</td>
<td>0</td>
<td>0</td>
<td>17</td>
<td>102</td>
<td>47.5%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Female</td>
<td>59</td>
<td>39</td>
<td>0</td>
<td>10</td>
<td>108</td>
<td>50.2%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No data</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>2.3%</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>357</td>
<td>Male</td>
<td>90</td>
<td>36</td>
<td>0</td>
<td>16</td>
<td>142</td>
<td>39.8%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Female</td>
<td>91</td>
<td>0</td>
<td>28</td>
<td>14</td>
<td>133</td>
<td>37.3%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No data</td>
<td>28</td>
<td>0</td>
<td>0</td>
<td>54</td>
<td>82</td>
<td>22.9%</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>213</td>
<td>Male</td>
<td>62</td>
<td>38</td>
<td>0</td>
<td>31</td>
<td>131</td>
<td>61.5%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Female</td>
<td>63</td>
<td>0</td>
<td>28</td>
<td>11</td>
<td>74</td>
<td>34.7%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No data</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>3.8%</td>
<td></td>
</tr>
</tbody>
</table>

In addition to the students, the teachers and parents were also surveyed as a way of triangulating issues such as the kinds of communication between the three participant groups in relation to perceived risks. All of the teachers who were surveyed (204) identified themselves as currently teaching middle school students (at least one of the four year levels). Similarly all of the parents/guardians (49) indicated that they had a child currently in the middle school. Table 3 indicates that the surveyed parents were distributed across the year levels with larger numbers in relation to year 9 which reflects the larger number of year 9 student responses.

Table 3
Distribution of parent survey participants by location and year level

<table>
<thead>
<tr>
<th>Location (Metropolitan and Independent)</th>
<th>Parents of Year 7</th>
<th>Parents of Year 8</th>
<th>Parents of Year 9</th>
<th>Parents of Year 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metropolitan (State and Independent)</td>
<td>4</td>
<td>4</td>
<td>16</td>
<td>2</td>
</tr>
<tr>
<td>Rural (State)</td>
<td>5</td>
<td>3</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>Total</td>
<td>9</td>
<td>7</td>
<td>22</td>
<td>11</td>
</tr>
</tbody>
</table>

No parents of students at Catholic schools responded to the surveys.
In addition to the surveys, the teachers were also interviewed with a particular focus on risk aversion strategies, educational use of SNS, and teacher perspectives of educational needs with regards to risk education. Finally, in an attempt to ensure that this research had identified all critical issues and risks a small number of experts in the fields of Australian law, teaching, child psychology and cybersafety were consulted. The experts were: Robyn Treyvaud, cybersafety education consultant; Professor Jock Given, Professor of Media and Communications at the Institute for Social Research (ISR), Swinburne University; and Melanie Saba, Chief Executive Officer at the Victorian Institute of Teaching.

3.2. **Surveys**

The surveys were anonymous and made available online and in paper based formats. The student, teacher and parent surveys had the same core questions as well as a number of questions specific to each participant group. The surveys used a mix of closed-ended questions (ordinal, Likert-scale and multiple choice) as well as open ended questions. While the ordinal questions allowed the researchers to quickly collect ranked data on participant SNS use and risk perceptions, it also posed a challenge in the analysis since the ordinal categories are known to often have indistinct or overly exclusionary boundaries or may have irregular distribution along a scale. For example, students were asked how often they updated or changed their SNS profile page. The possible answers were: several times a day, once a day, 3 to 5 times a week, 1 to 2 times a week, every few weeks or less often, never. While these categories have potential overlaps the wording was designed to be easily accessible for year 7 students through to adults (teachers and parents) while still providing a ranked comparison of SNS usage across the year levels. However, in order to strengthen the reliability of data analysis relating to ordinal questions, the categories are reported in full alongside the aggregated data, allowing the readers to make their own interpretations of ordinal significance in addition to that of the researchers.

All of the teacher and parent surveys were conducted online. The student surveys were primarily conducted online with 272 surveys administered in paper format. All of the paper format surveys were administered in state metropolitan schools and account for 43.3% of responses from those schools. The reason for offering paper based surveys was that not all schools can timetable student access to computer laboratories to complete the online surveys. The disadvantage of paper based surveys, however, is that students could choose to not answer questions or to provide answers which could not be used. As a result the total student responses vary across the questions. These variations are indicated in each table or discussion in the results.

3.3. **Interviews**

The focus group interviews of students and teachers were conducted during school time and on school premises. The focus group interviews were guided by, but not limited to, a set of questions relating to SNS practices and risks, either seeking further clarification of questions in the survey or probing for new issues or perspectives.

The researchers understood that interviews are not neutral data collection tools. The roles and relationships of the participants as well as the interviewer can affect the data collected. For instance, students may be purposely ambiguous about their SNS practices when talking with an adult. Similarly the teachers may be defensive or draw on language and attitudes which are
perceived to be suitable when talking to an ‘outsider’. In addition, there can be a tension between interviewers making a welcoming environment to share personal thoughts and feelings but also to remain sufficiently distant as to reduce influencing the participants’ stories.

Kvale 29 and Wolff 30 agree that the interviewer must project both an interest in what is being said but also an attitude of deliberate naïveté. If the interviewer reacts too strongly or personally to the content of the interview, or is evaluative, then it can sway the course of the interview and the way in which the content is phrased and interpreted. Consequently, this research adopted the recommendations of Hermanns 31: namely, to explain the context and structure of the interview to the subject, including the focus of the study; be relaxed and try to understand the meaning not just the words; give the subject room to open up; do not explain your views or dis/agree with them, do not be judgemental or evaluative, do not be protective of them; allow the story to unfold and do not dominate through high frequency of questions, interpretations, or even supportive utterances; use short accessible questions grounded in the terminology of the subject; and do not attempt to discover theoretical ideas but rather come to understand the life-world of the subject. These strategies were considered when designing the interview protocol.

3.4. Data Analysis

The survey data in each participant group was aggregated and in the case of students, analysed by year level, geographic location, and gender. Not all lines of analytic inquiry were useful and subsequently were not included in this report. The potential weakness of ordinal questions has already been discussed and is reduced through data triangulation with interviews and across participant groups. In the case of the open-ended questions which lent themselves to useful quantitative representation, an ordinal or categorical coding structure was developed based on the respondents’ answers. The subsequent coding was aggregated and reproduced in this report.

The interview data was transcribed, de-identified and coded according to themes in the survey questions (as a triangulation technique), and according to an iterative process which identified emergent themes from the surveys and interviews. In an attempt to increase reliability in the coding and analysis of interview data the four researchers independently analysed the same four transcripts, identifying themes relating to SNS practices, perceptions of risk, risk aversion strategies, and any other unexpected themes. The researchers then convened and negotiated a common understanding of the themes which would guide the remainder of the interview analysis.

4. Results:

Student SNS practices and perceptions of legal risk

This study surveyed 1004 middle school students (years 7-10), 204 middle school teachers and 49 parents of middle school students. In addition focus group interviews were conducted with 58 middle school students and 21 middle school teachers. The data was collected from 17 Victorian secondary schools from state (government run), Catholic and independent systems as well as metropolitan and rural locations (for details on the distribution of participants see Table 1, page 20).

4.1. The number of middle school students’ using SNS

The anonymous survey of 1004 middle school students found that 94.9% of those students reported using at least one SNS (see Table 4). Table 4 provides the frequency of students who use or do not use SNS according to school location and sector. This analysis also indicates that the usage of SNS by students from rural state schools (89.7%) is less than students from metropolitan state schools (97.7%). In addition, while the overwhelming usage of SNS by students in all non-rural schools is constant across the year levels, in rural schools there was a much larger proportion of students in year 7 who do not use SNS than in later years. Despite this difference between metropolitan and rural school students, and the variation within rural schools the survey results remain convincing in terms of the prevalence of SNS usage in all middle school years.

Table 4
Student participants: use of SNS, year level, system and location

<table>
<thead>
<tr>
<th>Year level</th>
<th>n</th>
<th>Students using SNS</th>
<th>Metropolitan</th>
<th>Catholic</th>
<th>Independent</th>
<th>Rural State</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>State</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>219</td>
<td>Yes</td>
<td>112</td>
<td>1</td>
<td>0</td>
<td>87</td>
<td>200</td>
<td>91.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>17</td>
<td>19</td>
<td>8.7</td>
</tr>
<tr>
<td>8</td>
<td>215</td>
<td>Yes</td>
<td>141</td>
<td>37</td>
<td>0</td>
<td>29</td>
<td>207</td>
<td>96.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>8</td>
<td>3.7</td>
</tr>
<tr>
<td>9</td>
<td>357</td>
<td>Yes</td>
<td>205</td>
<td>35</td>
<td>27</td>
<td>81</td>
<td>348</td>
<td>97.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>2.5</td>
</tr>
<tr>
<td>10</td>
<td>213</td>
<td>Yes</td>
<td>128</td>
<td>36</td>
<td>0</td>
<td>38</td>
<td>202</td>
<td>94.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>5</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>11</td>
<td>5.2</td>
</tr>
<tr>
<td>Total</td>
<td>1004</td>
<td>Yes</td>
<td>586</td>
<td>109</td>
<td>27</td>
<td>235</td>
<td>957</td>
<td>94.9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>14</td>
<td>5</td>
<td>1</td>
<td>27</td>
<td>47</td>
<td>5.1</td>
</tr>
</tbody>
</table>

The high usage of SNS by middle school students is known by their teachers and parents. Table 5 reveals that a remarkably similar percentage of parents (93.6%) and teachers (93.9%)
reported that their students/child currently used at least one SNS. This closely matches students’ reported usage of SNS (94.9%).

Table 5

<table>
<thead>
<tr>
<th></th>
<th>Students / child uses SNS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
</tr>
<tr>
<td>Teachers</td>
<td>204</td>
</tr>
<tr>
<td>Parents</td>
<td>49</td>
</tr>
<tr>
<td>Total</td>
<td>253</td>
</tr>
</tbody>
</table>

SNS are used equally by male (95.8%) and female (96.3%) middle school students (see Table 6). This is reflected across the year levels with similar percentages of males and females using SNS. The only difference being a slight depression of SNS usage in year 7 which has already been reported, but which reveals a slightly stronger usage of SNS by females.

Table 6

<table>
<thead>
<tr>
<th>Year level</th>
<th>n</th>
<th>Do you use SNS?</th>
<th>Male (n= 452)</th>
<th>Female (n=378)</th>
<th>Gender not recorded (n=174)</th>
<th>Total (n=1004)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>n</td>
<td>%</td>
<td>n</td>
<td>%</td>
</tr>
<tr>
<td>7</td>
<td>219</td>
<td>Yes</td>
<td>73</td>
<td>94.8</td>
<td>58</td>
<td>92.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>4</td>
<td>5.2</td>
<td>5</td>
<td>7.9</td>
</tr>
<tr>
<td>8</td>
<td>215</td>
<td>Yes</td>
<td>99</td>
<td>97.1</td>
<td>103</td>
<td>95.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>3</td>
<td>2.9</td>
<td>5</td>
<td>4.6</td>
</tr>
<tr>
<td>9</td>
<td>357</td>
<td>Yes</td>
<td>139</td>
<td>97.9</td>
<td>130</td>
<td>97.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>3</td>
<td>2.1</td>
<td>3</td>
<td>2.3</td>
</tr>
<tr>
<td>10</td>
<td>213</td>
<td>Yes</td>
<td>123</td>
<td>93.9</td>
<td>72</td>
<td>97.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>8</td>
<td>6.1</td>
<td>2</td>
<td>2.7</td>
</tr>
<tr>
<td>Total</td>
<td>1004</td>
<td>Yes</td>
<td>434</td>
<td>96.9</td>
<td>363</td>
<td>96.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>18</td>
<td>3.1</td>
<td>15</td>
<td>4.0</td>
</tr>
</tbody>
</table>

Table 6 also reveals that the surveys which did not report gender showed a slightly smaller percentage of students using SNS (92.0%) than either of the male (96.9%) or female (96%) averages. This difference can be explained by the fact that 79.3% of the surveys which did not indicate gender were from rural schools which have already been shown to have a lower usage rate. However, when each school sector or location was analysed according to gender, it was apparent that the percentage of males and females using SNS was very similar to one another and remained consistent across schools.

Despite the high level of student use of SNS it was surprising to note that in a separate question 26.9% of students stated that they have not created an online profile that others can see. This is interesting since all SNS, including Facebook (identified in Table 7 as the most popular SNS) require a profile in one form or another. The response suggests that many
students are unaware that the information about themselves which they place on a SNS can, when combined, constitute a profile.

4.2. **Specific SNS used by middle school students**

Facebook is the most popular SNS with 93.4% of students using it, followed by MySpace which was used by 26.6% of students (see Table 7). In response to the survey, students had indicated that they used 33 different sites which they felt were SNS. However, of those 33 sites the majority were found by the researchers to have social elements but did not meet the definition of SNS as described in the beginning of this report (in particular, many did not have the function to see other peoples’ networks). Table 7 lists the most popular SNS. It is interesting to note that many of the students used more than one SNS (ie. 864 students reported a total SNS frequency of 1160, 134.1%).

Table 7

*The most popular SNS used by students*

<table>
<thead>
<tr>
<th>SNS</th>
<th>Student (n=864)</th>
<th>Teacher (n=191)</th>
<th>Parent (n=46)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>%</td>
<td>n</td>
</tr>
<tr>
<td>Facebook</td>
<td>807</td>
<td>93.4</td>
<td>153</td>
</tr>
<tr>
<td>MySpace</td>
<td>230</td>
<td>26.6</td>
<td>91</td>
</tr>
<tr>
<td>Twitter</td>
<td>40</td>
<td>4.6</td>
<td>15</td>
</tr>
<tr>
<td>Bebo</td>
<td>40</td>
<td>4.6</td>
<td>4</td>
</tr>
<tr>
<td>Tumblr</td>
<td>22</td>
<td>2.5</td>
<td>1</td>
</tr>
<tr>
<td>Formspring</td>
<td>13</td>
<td>1.5</td>
<td>1</td>
</tr>
<tr>
<td>YouTube</td>
<td>8</td>
<td>0.9</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>1160</td>
<td>134.1</td>
<td>264</td>
</tr>
</tbody>
</table>

*There were 957 students who indicated that they used a SNS. However, 93 of these students did not specify the SNS they used. This table also includes all teachers and parents who indicated that they knew their students/children used SNS.

**32 sites were mentioned by students of which most did not meet the definition of SNS. In addition to those listed in Table 7 the following sites were identified by students as SNS: MSN Instant Messenger (122), Skype (8), Deviantart (5), Xbox live (5), Tagged (5), Steam (3), Gmail (2), Google Buzz (2), Blogspot (2), Chat roulette (2), Flikr (2), Chacha.me (2), Yahoo Answers (2), Sns fun (2), Gaia online (2), Dailybooth (1), Orkut (1), Picasa (1), Friendster (1), Ping (1), Omegle (1), Mweor (1), Second Life (1), Friends 21 (1), Bearshare (1), Miniclip (1).

Table 7 also indicates that Teachers and Parents were aware that students/children not only used but also preferred Facebook over MySpace and that they used more than one SNS. Four teachers commented that their students use “all of them” and a parent stated: “you name it, it is used or tried out.” Nevertheless, despite the awareness of teachers and parents of the most popular SNS, they did not identify many of the less popular sites which students used. Indeed, only one teacher and two parents reported that “there may be others that I do not know about.”

When considering the four most popular SNS used by students the distribution across the year levels is similar (see Table 8 and Figure 1). It is interesting to note that while Facebook was consistently the most popular SNS, its popularity was similar in Years 7 to 9 but dropped slightly in Year 10. Years 8 and 10 used MySpace more than the other years but also indicated that they were more likely to use more than one SNS (both years had over 140% usage of SNS).
Table 8
The most popular SNS used by students by year level

<table>
<thead>
<tr>
<th>SNS</th>
<th>Year 7 (n=197)</th>
<th>Year 8 (n=205)</th>
<th>Year 9 (n=269)</th>
<th>Year 10 (n=193)</th>
<th>Total (n=864)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>%</td>
<td>n</td>
<td>%</td>
<td>n</td>
</tr>
<tr>
<td>Facebook</td>
<td>188</td>
<td>95.4</td>
<td>193</td>
<td>94.1</td>
<td>253</td>
</tr>
<tr>
<td>MySpace</td>
<td>34</td>
<td>17.3</td>
<td>87</td>
<td>42.4</td>
<td>46</td>
</tr>
<tr>
<td>Twitter</td>
<td>1</td>
<td>0.5</td>
<td>6</td>
<td>2.9</td>
<td>6</td>
</tr>
<tr>
<td>Bebo</td>
<td>0</td>
<td>0.0</td>
<td>13</td>
<td>6.3</td>
<td>15</td>
</tr>
<tr>
<td>Total</td>
<td>223</td>
<td>113.2</td>
<td>299</td>
<td>145.9</td>
<td>320</td>
</tr>
</tbody>
</table>

Table 8 indicates that 95.4% of year 7 students used Facebook. This is noteworthy since Facebook has a minimum age of 13 but year 7 students can be aged between 12 and 14. However, since the ages of students were not collected we can only speculate that some students may ignore age restrictions in SNS Terms of Service agreements. The only indication of students being conscious of age restrictions was reported by one student in the focus group interviews who commented: “I had to wait until I was 13. I’m 13 now, but my mum [still] just sort of wants me, I guess, to wait” however the same student indicated that while she was “not unhappy or anything” she still intended to join Facebook in the near future. Further investigation of age and awareness and response to age restrictions of SNS may be valuable in future studies.

How students choose which SNS to use

Students were asked to explain how they chose which social networking sites to use. 45% indicated that their friends were a significant factor with typical responses being: “Whatever [sic] one my friends’ use” and “what my mates had because the whole reason is to socialize with them”. An additional 30% did not specify their friends but indicated they chose the SNS
because they thought it was popular (presumably either with their peer group or through popular media), for example, “I reckon everybody likes to use it because it’s popular and people know of it.” Only 6% of students indicated that family were an important factor when choosing SNS, for example “because my family has Facebook so I did the same”. Finally, only 5% of students reported that they gave the choice little thought, for example “eeny meeny mynie moe” and “dunno” being representative. The remaining 14% of students did not answer the question.

One of the students in the focus group interviews also highlighted the potential influence of commercial interests: “Facebook is becoming almost like a marketing thing now, because lots of people use Facebook, phone companies go, ‘Here, 300 hours of free Facebook with this sim card and you get this phone as well, with this plan.’ It’s just a marketing thing now, Facebook and Twitter.”

4.3. Frequency of middle phase students using SNSs

Students were asked to indicate how frequently they edited their SNS profile. Table 9 reveals that the majority of students update information on their SNS on a daily basis and that over a quarter of students in each year level update their SNS profile several times a day.

Table 9
Frequency of students updating their own SNS by year level

<table>
<thead>
<tr>
<th>Frequency of updates</th>
<th>Year 7 (n=199)</th>
<th>Year 8 (n=205)</th>
<th>Year 9 (n=329)</th>
<th>Year 10 (n=191)</th>
<th>Total (n=924)</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>%</td>
<td>n</td>
<td>%</td>
<td>n</td>
<td>%</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Several times each day</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>30.6</td>
<td>54</td>
<td>26.3</td>
<td>101</td>
<td>30.7</td>
</tr>
<tr>
<td>About once a day</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>31.7</td>
<td>62</td>
<td>30.2</td>
<td>93</td>
<td>28.3</td>
</tr>
<tr>
<td>3 to 5 times per week</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>13.6</td>
<td>34</td>
<td>16.6</td>
<td>46</td>
<td>14.0</td>
</tr>
<tr>
<td>1 or 2 times per week</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>11</td>
<td>28</td>
<td>13.7</td>
<td>51</td>
<td>15.5</td>
</tr>
<tr>
<td>Every few weeks, less often</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>13.1</td>
<td>27</td>
<td>13.2</td>
<td>38</td>
<td>11.5</td>
</tr>
<tr>
<td>Total</td>
<td>199</td>
<td>205</td>
<td>329</td>
<td>191</td>
<td>924</td>
</tr>
</tbody>
</table>

A general trend, illustrated in Figure 2, is that the frequency of updating SNS increases across the year levels. Indeed, three quarters of year 10 students (75.3%, see Table 9) update their SNS at least once every day. This increase is partly explained by the way in which the SNS are used by the different year levels. The next section reveals that, in general, older year levels increasingly use the SNS for regular communication purposes which in turn means they need to access their SNS more often.
When the students’ frequency of updating their own SNS is analysed according to year level and gender it is apparent that similar proportions of both male and female students in each year level have the same frequency of usage (see Table 10).
Table 10
Frequency of students updating their own SNS by year level and gender

<table>
<thead>
<tr>
<th>Students</th>
<th>Several times a day</th>
<th>About once a day</th>
<th>3 to 5 times per week</th>
<th>1 or 2 times per week</th>
<th>Every few weeks, less often</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>n=75</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>n 21</td>
<td>20</td>
<td>13</td>
<td>8</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>% 28</td>
<td>26.7</td>
<td>17.3</td>
<td>10.7</td>
<td>17.3</td>
</tr>
<tr>
<td>Female</td>
<td>(n=63)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>n 18</td>
<td>20</td>
<td>9</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>% 28.6</td>
<td>31.7</td>
<td>14.3</td>
<td>11.1</td>
<td>14.3</td>
</tr>
<tr>
<td>Year 8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>(n=97)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>n 26</td>
<td>29</td>
<td>15</td>
<td>14</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>% 26.8</td>
<td>29.9</td>
<td>15.5</td>
<td>14.4</td>
<td>13.4</td>
</tr>
<tr>
<td>Female</td>
<td>(n=103)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>n 27</td>
<td>31</td>
<td>18</td>
<td>14</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>% 26.2</td>
<td>30.1</td>
<td>17.5</td>
<td>13.6</td>
<td>12.6</td>
</tr>
<tr>
<td>Year 9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>(n=130)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>n 39</td>
<td>36</td>
<td>19</td>
<td>20</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>% 30</td>
<td>27.7</td>
<td>14.6</td>
<td>15.4</td>
<td>12.3</td>
</tr>
<tr>
<td>Female</td>
<td>(n=122)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>n 38</td>
<td>35</td>
<td>17</td>
<td>19</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>% 31.1</td>
<td>28.7</td>
<td>13.9</td>
<td>15.6</td>
<td>10.7</td>
</tr>
<tr>
<td>Year 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>(n=116)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>n 39</td>
<td>47</td>
<td>10</td>
<td>9</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>% 33.6</td>
<td>40.5</td>
<td>8.6</td>
<td>7.8</td>
<td>9.5</td>
</tr>
<tr>
<td>Female</td>
<td>(n=68)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>n 22</td>
<td>31</td>
<td>5</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>% 32.4</td>
<td>45.6</td>
<td>7.4</td>
<td>4.4</td>
<td>10.3</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>(n=418)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>n 125</td>
<td>132</td>
<td>57</td>
<td>51</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>% 29.9</td>
<td>31.6</td>
<td>13.6</td>
<td>12.2</td>
<td>12.7</td>
</tr>
<tr>
<td>Female</td>
<td>(n=356)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>n 105</td>
<td>117</td>
<td>49</td>
<td>43</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>% 29.5</td>
<td>32.9</td>
<td>13.8</td>
<td>12.1</td>
<td>11.8</td>
</tr>
</tbody>
</table>

*The totals are different from the previous table because responses which did not indicate gender were excluded (i.e. 957 students reported that they used a SNS but only 797 indicated their gender). In addition 23 students did not answer the question which leaves 774 valid responses to this question.*

Figure 4. Average frequency of male and female students updating their own SNS.
4.4. **What students do with SNS**

The many SNS available to students provide a large number of different activities including playing games (such as Farmville in Facebook), creating photo albums, participating in a variety of surveys, identifying their likes and dislikes, and so on. This research has not attempted to quantify all student activities in SNS. Instead, the researchers decided to inquire into the purposeful way in which students use SNS to engage with each other, to better understand the social context which makes SNS different from other Web 2.0 applications.

Overall students indicated that they used SNS to communicate with current friends and especially to stay in touch with friends they rarely see in person (see Table 11).

Table 11

*The activities for which students use SNS*

<table>
<thead>
<tr>
<th>What are SNS used for?#</th>
<th>Student (n=900)##</th>
<th>Teacher (n=191)</th>
<th>Parent (n=46)</th>
</tr>
</thead>
<tbody>
<tr>
<td>To make new friends</td>
<td>365 41.0</td>
<td>124 64.9</td>
<td>9 19.6</td>
</tr>
<tr>
<td>To stay in touch with friends they see a lot</td>
<td>692 77.8</td>
<td>186 97.4</td>
<td>44 95.7</td>
</tr>
<tr>
<td>To stay in touch with friends they rarely see in person</td>
<td>809 90.6</td>
<td>124 64.9</td>
<td>32 69.6</td>
</tr>
<tr>
<td>To flirt with someone</td>
<td>223 24.8</td>
<td>116 60.7</td>
<td>8 17.4</td>
</tr>
<tr>
<td>To make plans with friends</td>
<td>689 76.6</td>
<td>168 88.0</td>
<td>33 71.7</td>
</tr>
</tbody>
</table>

# These categories were guided by themes from the research literature and popular media. Options 1 and 4 are often portrayed as having elements of risk or danger while options 2, 3 and 5 are usually seen as benign.

## 957 students indicated that they used SNS. However, 57 of these students did not answer this question. This table also includes all teachers and parents who indicated that they knew their students/children used SNS.

However, Figure 5 helps to reveal that Teachers believe students use SNS to make new friends and to flirt at a much higher frequency than reported by students. Parents however have an impression that their children use SNS to make new friends and to flirt at a lower frequency than reported by students.
The variation between students and their parents and teachers in regard to the reported frequency of using SNS to keep in contact with friends who they see a lot or see rarely is notable and may reflect students’ different perceptions of “a lot” and “rarely” from their teachers and parents.

Table 12 (illustrated in Figure 6) clearly indicates that SNS are primarily used to maintain current networks (staying in touch and planning with friends). Expanding the network (making new friends) and sexual interaction (flirting) were relatively low in students’ reported practices. However there is an exception to this pattern in the year 7 students’ responses. Year 7 students indicated a noticeably lower frequency of using SNS to stay in touch with friends they see “a lot”. This is particularly obvious when illustrated graphically (see Figure 6). This anomaly cannot be explained without significant conjecture, nevertheless the conclusion that SNS are primarily used to maintain networks is supported since a high percentage of year 7 students (86.2%) indicated that they used SNS to stay in touch with friends they “rarely” see.

Table 12
The activities for which students by year level use SNS

<table>
<thead>
<tr>
<th></th>
<th>Year 7 (n=196)</th>
<th>Year 8 (n=192)</th>
<th>Year 9 (n=322)</th>
<th>Year 10 (n=190)</th>
<th>Total (n=900)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n  %</td>
<td>n  %</td>
<td>n  %</td>
<td>n  %</td>
<td>n  %</td>
</tr>
<tr>
<td>To make new friends?</td>
<td>84  42.9</td>
<td>74  38.5</td>
<td>119 37.0</td>
<td>88  46.3</td>
<td>365 40.6</td>
</tr>
<tr>
<td>To stay in touch with a lot</td>
<td>59  30.1</td>
<td>170 88.5</td>
<td>287 89.1</td>
<td>176 92.6</td>
<td>692 76.9</td>
</tr>
<tr>
<td>To stay in touch with friends you rarely see in person</td>
<td>169 86.2</td>
<td>174 90.6</td>
<td>282 87.6</td>
<td>184 96.8</td>
<td>809 89.9</td>
</tr>
<tr>
<td>To flirt with someone?</td>
<td>48  24.5</td>
<td>44 22.9</td>
<td>81 25.2</td>
<td>50  26.3</td>
<td>223 24.8</td>
</tr>
<tr>
<td>To make plans with your friends?</td>
<td>135 68.9</td>
<td>167 87.0</td>
<td>234 72.7</td>
<td>153 80.5</td>
<td>689 76.6</td>
</tr>
</tbody>
</table>

*357 students indicated that they used SNS. 57 of those students did not answer this question.
Both male and female students use SNS for similar purposes. Table 13 reveals a general trend that similar percentages of male and female students in each year level use the SNS for similar purposes. However, Figure 7 helps to illustrate that, with few exceptions a larger percentage of female students use SNS for these purposes, especially to stay in contact with friends they “rarely” see and to make plans with friends.

Table 13
The activities for which students by year level use SNS by gender

<table>
<thead>
<tr>
<th>Gender</th>
<th>Year 7 (m=73, f=58)</th>
<th>Year 8 (m=99, f=103)</th>
<th>Year 9 (m=139, f=130)</th>
<th>Year 10 (m=123, f=72)</th>
<th>Total (m=434, f=363)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>%</td>
<td>n</td>
<td>%</td>
<td>n</td>
</tr>
<tr>
<td>To make new friends?</td>
<td>Male</td>
<td>28</td>
<td>38.4</td>
<td>35</td>
<td>35.4</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>31</td>
<td>53.4</td>
<td>38</td>
<td>36.9</td>
</tr>
<tr>
<td>To stay in touch with friends you see a lot?</td>
<td>Male</td>
<td>23</td>
<td>31.5</td>
<td>82</td>
<td>82.8</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>20</td>
<td>34.5</td>
<td>85</td>
<td>82.5</td>
</tr>
<tr>
<td>To stay in touch with friends you rarely see in person?</td>
<td>Male</td>
<td>64</td>
<td>87.7</td>
<td>80</td>
<td>80.8</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>57</td>
<td>98.3</td>
<td>91</td>
<td>88.4</td>
</tr>
<tr>
<td>To flirt with someone?</td>
<td>Male</td>
<td>15</td>
<td>20.6</td>
<td>20</td>
<td>20.2</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>17</td>
<td>29.3</td>
<td>24</td>
<td>23.3</td>
</tr>
<tr>
<td>To make plans with your friends?</td>
<td>Male</td>
<td>48</td>
<td>65.8</td>
<td>79</td>
<td>79.8</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>47</td>
<td>81.0</td>
<td>86</td>
<td>83.5</td>
</tr>
</tbody>
</table>
In addition the 46 parents who indicated they knew their child used SNS were asked if they believed their child used SNS to stay in touch with family. In response, 23 parents (50%) indicated that their child did stay in touch with family through SNS. This also implies that family members are included in the child’s SNS networks and presumably can see their profile. However, the survey did not disclose the particular familial relationships involved which means it could have been sibling or other younger family members rather than adults.

In a similar triangulating question the same 46 parents were asked if they communicated with their child/ward using a SNS. The answers are represented in Figure 8. In response, 17 parents (36.9%) indicated that they “frequently” or “regularly” used SNS to communicate or interact with their child/ward. A further 5 parents (10.9%) reported infrequent communication through SNS such as: “Only when she was away on holidays”, “Reminders from time to time to be careful and not to elicit or click on new people”. In total 22 parents (47.8%) communicated
with their child/ward using SNS and therefore were included in the child’s SNS networks and presumably could see their profile. However, 24 parents (52.2%) reported that they did not use SNS to communicate with their child/ward. The explanations included purposeful exclusion by their child/ward such as “no, because I am not permitted to be a friend”, parents’ own lack of engagement with the technology such as “no, I do not use any social networks on computer”, and implied value judgements such as “No. I’m afraid I communicate with my child through talk and body language. And sometimes the phone.”

![Figure 8. Frequency of parents communicating with their child via SNS.](image)

Although over half of parents did not communicate with their child/ward through SNS, 37 parents (80.4% of the 46 parents who indicated that their child uses SNS) indicated that they had seen their child/ward’s SNS profile. Of the 37 parents 9 reported they “were a little concerned with what they saw”, 3 reported they were “very concerned with what they saw” and 25 reported they were “happy with what they saw”.

This research also quantified the ways in which students communicated or interacted with their network according to common social interaction functions available in the popular SNS.

Table 14 reveals that middle school students were more likely to use SNS to post public messages on ‘friends’ pages or blogs and to send private messages than to upload images, send group messages or initiate a notification such as a ‘poke’. In addition, Figure 9 illustrates that more year 9 students indicated that they were more likely to use a variety of SNS communication functions when compared with other students.
Table 14
Methods of student communication with friends using SNS by year level

<table>
<thead>
<tr>
<th>Type of communication</th>
<th>Year 7 (n=200)</th>
<th>Year 8 (n=207)</th>
<th>Year 9 (n=348)</th>
<th>Year 10 (n=202)</th>
<th>Total (n=957)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>%</td>
<td>n</td>
<td>%</td>
<td>n</td>
</tr>
<tr>
<td>Post messages to a friend's page or wall</td>
<td>84</td>
<td>42.0</td>
<td>74</td>
<td>35.8</td>
<td>248</td>
</tr>
<tr>
<td>Post photos/ images to a friends' page or wall</td>
<td>54</td>
<td>27.0</td>
<td>42</td>
<td>20.3</td>
<td>149</td>
</tr>
<tr>
<td>Send a bulletin or group message to all of your friends</td>
<td>27</td>
<td>9.8</td>
<td>16</td>
<td>7.7</td>
<td>69</td>
</tr>
<tr>
<td>Send private messages to a friend within the social networking system</td>
<td>80</td>
<td>40.0</td>
<td>75</td>
<td>36.2</td>
<td>242</td>
</tr>
<tr>
<td>Wink, poke, give 'e-props' or kudos to your friends</td>
<td>36</td>
<td>18.0</td>
<td>36</td>
<td>17.4</td>
<td>95</td>
</tr>
<tr>
<td>Post comments to a friend's blog</td>
<td>63</td>
<td>31.5</td>
<td>46</td>
<td>22.2</td>
<td>142</td>
</tr>
</tbody>
</table>

*The categories for types of communication were based on functions available in the most common SNS.*

Figure 9. Methods of student communication with friends using SNS.

When the data is analysed according to year level and gender it becomes apparent that in most uses of SNS communication functions both male and female students are very similar within a year level and across year levels (see Table 15). This pattern is marginally different in two cases as illustrated by Figure 10. Male students in years 7 to 10 are more likely post
photos to a friend’s page/wall than females. In contrast, female students in years 7 to 10 are more likely to send private messages to friends.

Table 15
Methods of student communication using SNS by year level and gender

<table>
<thead>
<tr>
<th>Type of communication</th>
<th>Gender</th>
<th>Year 7 (m=n=75)</th>
<th>Year 8 (m=n=99)</th>
<th>Year 9 (m=n=140)</th>
<th>Year 10 (m=n=128)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>m (n=61)</td>
<td>f (n=61)</td>
<td>m (n=101)</td>
<td>f (n=101)</td>
</tr>
<tr>
<td>Post messages to a friend’s page or wall</td>
<td>Male</td>
<td>29 50.9</td>
<td>35 35.4</td>
<td>99 70.7</td>
<td>53 39.1</td>
</tr>
<tr>
<td>Post photos / images to a friend’s page or wall</td>
<td>Male</td>
<td>22 38.6</td>
<td>21 21.2</td>
<td>67 47.9</td>
<td>26 20.3</td>
</tr>
<tr>
<td>Send a bulletin or group message to all of your friends</td>
<td>Male</td>
<td>9 15.8</td>
<td>7 7.1</td>
<td>27 19.3</td>
<td>16 12.5</td>
</tr>
<tr>
<td>Send private messages to a friend within the social networking system</td>
<td>Male</td>
<td>24 42.1</td>
<td>31 31.3</td>
<td>93 66.4</td>
<td>50 39.1</td>
</tr>
<tr>
<td>Wink, poke, give 'e-props' or kudos to your friends</td>
<td>Male</td>
<td>13 22.8</td>
<td>17 17.2</td>
<td>31 22.1</td>
<td>20 15.6</td>
</tr>
<tr>
<td>Post comments to a friend’s blog</td>
<td>Male</td>
<td>22 38.6</td>
<td>22 22.2</td>
<td>60 42.9</td>
<td>26 20.3</td>
</tr>
</tbody>
</table>

Figure 10. Comparison of male and female students’ use of SNS communication tools

4.5. The content which students post to SNS

In addition to the ways in which students communicate with others via SNS, this research gathered information regarding the kinds of content students upload to their own SNS in
addition to status updates. This is particularly relevant in describing the context within which legal risks can be found such as copyright infringement and disclosure. Table 16 indicates that the most common content posted is photos of themselves (60.9%), closely followed by photos of their friends (52.6%). While posting third party music, video and pictures of others such as celebrities are less popular, these activities are still well represented, for instance while an average of 38.5% of students reported that they posted videos the proportion rises to 69.8% for year 10 students.

Table 16

<table>
<thead>
<tr>
<th>Types of SNS content posted by students by year level</th>
<th>Year 7 (n=200)</th>
<th>Year 8 (n=207)</th>
<th>Year 9 (n=348)</th>
<th>Year 10 (n=202)</th>
<th>Total (n=957)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pictures of me</td>
<td>90  45.0</td>
<td>83  40.1</td>
<td>244  70.1</td>
<td>166  82.2</td>
<td>583  60.9</td>
</tr>
<tr>
<td>Pictures of my friends</td>
<td>75  37.5</td>
<td>68  32.9</td>
<td>213  61.2</td>
<td>147  72.8</td>
<td>503  52.6</td>
</tr>
<tr>
<td>Music</td>
<td>40  20.0</td>
<td>68  32.9</td>
<td>94  27.0</td>
<td>72  35.6</td>
<td>255  26.7</td>
</tr>
<tr>
<td>Other pictures (eg. celebrities)</td>
<td>24  12.0</td>
<td>14  6.8</td>
<td>24  6.9</td>
<td>29  14.4</td>
<td>91  9.5</td>
</tr>
<tr>
<td>Videos (eg. movie clips, links to YouTube)</td>
<td>62  31.0</td>
<td>33  15.9</td>
<td>132  37.9</td>
<td>141  69.8</td>
<td>368  38.5</td>
</tr>
</tbody>
</table>

Figure 11. Types of SNS content posted by students.

Male and female students within the same year level reported similar frequencies in the types of content posted on their SNS (see Table 17).
Table 17
Types of SNS content posted by students by year level and gender

<table>
<thead>
<tr>
<th>Type of content</th>
<th>Gender</th>
<th>Year 7 m (n=75)</th>
<th>Year 8 m (n=99)</th>
<th>Year 9 m (n=140)</th>
<th>Year 10 m (n=128)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>n (%)</td>
<td>n (%)</td>
<td>n (%)</td>
<td>n (%)</td>
</tr>
<tr>
<td>Pictures of me</td>
<td>Male</td>
<td>30 40.0</td>
<td>39 39.4</td>
<td>97 69.3</td>
<td>100 78.1</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>26 42.6</td>
<td>42 41.6</td>
<td>98 74.8</td>
<td>58 80.6</td>
</tr>
<tr>
<td>Pictures of my friends</td>
<td>Male</td>
<td>26 34.7</td>
<td>33 33.3</td>
<td>84 60.0</td>
<td>91 71.1</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>20 32.8</td>
<td>34 33.7</td>
<td>86 65.7</td>
<td>50 69.4</td>
</tr>
<tr>
<td>Music</td>
<td>Male</td>
<td>14 6.5</td>
<td>23 23.2</td>
<td>37 26.4</td>
<td>45 35.2</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>11 18.0</td>
<td>23 22.8</td>
<td>35 26.7</td>
<td>25 34.7</td>
</tr>
<tr>
<td>Other pictures (eg. celebrities)</td>
<td>Male</td>
<td>9 12.0</td>
<td>6 6.1</td>
<td>10 7.1</td>
<td>17 13.3</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>9 14.8</td>
<td>6 5.9</td>
<td>9 6.9</td>
<td>10 13.9</td>
</tr>
<tr>
<td>Videos (eg. movie clips, links to YouTube)</td>
<td>Male</td>
<td>25 30.0</td>
<td>15 15.2</td>
<td>52 37.1</td>
<td>96 75.0</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>15 24.6</td>
<td>16 15.8</td>
<td>48 36.6</td>
<td>40 55.6</td>
</tr>
</tbody>
</table>

Figure 12. Year 7 types of content posted to their SNS.

Figure 13. Year 8 types of content posted to their SNS.
Figure 14. Year 9 types of content posted to their SNS.

Figure 15. Year 10 types of content posted to their SNS.

One of the defining characteristics of middle school students, or more accurately adolescence, is their exploration and negotiation of identity. SNS have been claimed as sites of identity construction and reconstruction, wherein the content posted to a SNS profile and the forms of engagement between that profile and others shapes an online identity. This research gathered evidence of whether students were aware of the relationship between their online SNS profile and their perceived ‘real-life’ identity.

Table 18 indicates that the majority of year 7 to 10 students (67.6%) believed their SNS is either an exact or partial reflection of themselves. In addition, 11.3% indicated that it showed an idealised version of themselves.
Table 18
*Do SNS profiles accurately reflect student identity (year)*

<table>
<thead>
<tr>
<th></th>
<th>Year 7 (n=199)</th>
<th>Year 8 (n=200)</th>
<th>Year 9 (n=324)</th>
<th>Year 10 (n=188)</th>
<th>Total (n=911)</th>
</tr>
</thead>
<tbody>
<tr>
<td>It reflects exactly who I am</td>
<td>n</td>
<td>%</td>
<td>n</td>
<td>%</td>
<td>n</td>
</tr>
<tr>
<td>Year 7</td>
<td>70</td>
<td>35.2</td>
<td>62</td>
<td>31.0</td>
<td>97</td>
</tr>
<tr>
<td>Year 8</td>
<td>52</td>
<td>26.1</td>
<td>62</td>
<td>31.0</td>
<td>143</td>
</tr>
<tr>
<td>Year 9</td>
<td>24</td>
<td>12.1</td>
<td>26</td>
<td>13.0</td>
<td>44</td>
</tr>
<tr>
<td>Year 10</td>
<td>53</td>
<td>26.6</td>
<td>50</td>
<td>25.0</td>
<td>40</td>
</tr>
<tr>
<td>Total</td>
<td>199</td>
<td>100</td>
<td>200</td>
<td>100</td>
<td>324</td>
</tr>
</tbody>
</table>

*This table reports on 911 students (out of 957 students who used SNS) who answered this question.*

**Figure 16.** Do SNS profiles accurately reflect student identity (year)

A significant proportion of the students (21.1%) used the open ended option of “other” to provide alternative explanations, indicating that the SNS was not a reflection of themselves. However, the explanations varied in strength and credibility. Some students discounted the notion that their SNS profile had any relationship to their identity, for example:

- “It’s just a place that I use to send and receive information”,
- “I use Facebook, I don’t make a 'profile' showing what I am like. It just has information about me”
- “It has no great reflection on me apart from who I am friends with as I interact with them on my wall.”

[41]
Clearly the credibility of these claims are in question since the persistent record of interaction and activity combined with the SNS profiling of name and other information necessarily creates an identity. However, other students stated that their SNS profile either did not reflect them or elements of truth were dominated by fiction, for example:

- “It’s reminds me of a phoney, its me, but i don’t do things i would do to be myself”,
- “um, its a website.....? everyone knows its not you”,
- “i lie about everything, nothing on my profile is true”,
- “I put down my basic personality and make myself appear exaggeratedly insane. What fun.”

When the data is analysed according to gender there is little variation in the pattern (see Table 19). Male and female students within the same year level have a similar perception of the accuracy of the SNS reflecting who they are. The only notable variation (illustrated in Figure 17) is in year 9 and especially in year 10 where a higher percentage of females reported their SNS is an exact or partial reflection. In contrast more males indicated that that their SNS was not a reflection of themselves. This pattern is reversed in years 7 and 8.

Table 19
Do SNS profiles accurately reflect student identity (year and gender)

<table>
<thead>
<tr>
<th>Accuracy of reflected identity</th>
<th>Gender</th>
<th>Year 7 m (n=75)</th>
<th>Year 8 m (n=93)</th>
<th>Year 9 m (140)</th>
<th>Year 10 m (116)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>f (n=63)</td>
<td>f (101)</td>
<td>f (n=122)</td>
<td>f (n=65)</td>
</tr>
<tr>
<td>It reflects exactly who I am</td>
<td>Male</td>
<td>26 34.7</td>
<td>29 31.2</td>
<td>37 26.4</td>
<td>23 19.8</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>21 33.3</td>
<td>31 30.7</td>
<td>35 28.7</td>
<td>19 29.2</td>
</tr>
<tr>
<td>It reflects some but not all of who I am</td>
<td>Male</td>
<td>22 29.3</td>
<td>29 31.2</td>
<td>56 40.0</td>
<td>47 40.5</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>16 25.4</td>
<td>29 28.7</td>
<td>53 43.4</td>
<td>31 47.7</td>
</tr>
<tr>
<td>It shows an idealised version of me (e.g. it is what I want my friends to think I am like)</td>
<td>Male</td>
<td>14 18.7</td>
<td>17 18.3</td>
<td>26 18.6</td>
<td>11 9.5</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>13 20.6</td>
<td>21 20.8</td>
<td>17 13.9</td>
<td>5 7.7</td>
</tr>
<tr>
<td>Other (e.g. SNS is not a reflection of who I am)</td>
<td>Male</td>
<td>13 17.3</td>
<td>18 19.4</td>
<td>21 15.0</td>
<td>35 30.2</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>13 20.6</td>
<td>20 19.8</td>
<td>17 13.9</td>
<td>10 15.4</td>
</tr>
</tbody>
</table>

[42]
As a process of data triangulation students were also asked to identify the types of content posted to SNS by their friends. The pattern was similar to that of their own responses, indicating that they saw their own content creation in SNS to be similar to that of their social network. One of the interesting findings of this question was that 45.6% of students reported that their photos had been posted on their friends’ SNS. In addition, 62.1% of students reported that photos of their friends had been posted on other people’s SNS.

Table 20

<table>
<thead>
<tr>
<th>Types of SNS content posted by students’ friends</th>
<th>Year 7 (n=201)</th>
<th>Year 8 (n=197)</th>
<th>Year 9 (n=322)</th>
<th>Year 10 (n=185)</th>
<th>Total (n=905)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pictures of me</td>
<td>n</td>
<td>%</td>
<td>n</td>
<td>%</td>
<td>n</td>
</tr>
<tr>
<td>Pictures of my friends</td>
<td>73</td>
<td>36.3</td>
<td>58</td>
<td>29.4</td>
<td>210</td>
</tr>
<tr>
<td>Music</td>
<td>96</td>
<td>47.8</td>
<td>86</td>
<td>43.7</td>
<td>283</td>
</tr>
<tr>
<td>Other pictures (eg. celebrities)</td>
<td>46</td>
<td>22.9</td>
<td>54</td>
<td>27.4</td>
<td>145</td>
</tr>
<tr>
<td>Videos (eg. movies clips, links to YouTube)</td>
<td>62</td>
<td>30.9</td>
<td>46</td>
<td>23.4</td>
<td>178</td>
</tr>
<tr>
<td>Other</td>
<td>27</td>
<td>13.4</td>
<td>29</td>
<td>14.7</td>
<td>64</td>
</tr>
</tbody>
</table>
Since there are increasing concerns of issues of disclosure through posting of images the survey asked students if they felt concerned about their images being posted by others on their friend’s SNS. Overall 80.3% of students were not concerned. However, 19.7% indicated that they were concerned with this practice (see Table 21).

Table 21
Are students concerned when their images are posted on friends’ SNS?

<table>
<thead>
<tr>
<th></th>
<th>Year 7 (n=197)</th>
<th>Year 8 (n=204)</th>
<th>Year 9 (n=343)</th>
<th>Year 10 (n=190)</th>
<th>Total (n=934)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n   %</td>
<td>n   %</td>
<td>n   %</td>
<td>n   %</td>
<td>n   %</td>
</tr>
<tr>
<td>Yes</td>
<td>44 22.3</td>
<td>48 23.5</td>
<td>57 16.6</td>
<td>35 18.4</td>
<td>184 19.7</td>
</tr>
<tr>
<td>No</td>
<td>153 77.7</td>
<td>156 76.5</td>
<td>286 83.4</td>
<td>155 81.6</td>
<td>750 80.3</td>
</tr>
</tbody>
</table>

4.6. The value of SNS

The data already discussed clearly indicates that SNS are embedded in the vast majority of years 7-10 students’ lives. They use SNS to frequently engage with their networks of ‘friends’, often updating or adding to their SNS pages. In an attempt to further understand the significance of SNS in students’ lives the survey included an open ended question asking students to describe if SNS were important to them. Table 22 presents a frequency count based on a coding of the 842 responses. Considering the popularity and frequency of use of SNS it is perhaps not surprising that only 6.3% of students indicated that SNS were not important to them. In contrast, 33.4% of students were strongly affirmative about the importance of SNS. However, this should be put into context of the 62.6% of students who reported that they updated their SNS at least once a day (see Table 9). The implication is that while updating SNS is a daily activity for most students, many of them do not perceive it to be very important. The majority of students (60.3%, Table 22) affirmed, not strongly affirmed, that SNS had some value to them. For these students most of the responses which provided detail either suggested the students saw SNS as a useful communication tool, or for stimulation when “bored”.

Table 22
The importance of SNS to students

<table>
<thead>
<tr>
<th></th>
<th>Year 7 (n=192)</th>
<th>Year 8 (n=178)</th>
<th>Year 9 (n=289)</th>
<th>Year 10 (n=183)</th>
<th>Total (n=842)*</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n   %</td>
<td>n   %</td>
<td>n   %</td>
<td>n   %</td>
<td>n   %</td>
</tr>
<tr>
<td>Strongly affirmative response (eg. “very important”)</td>
<td>76 39.6</td>
<td>64 36.0</td>
<td>85 29.4</td>
<td>56 30.6</td>
<td>281 33.4</td>
</tr>
<tr>
<td>Affirmative response (eg. &quot;only important for keeping contact with friends&quot;, “not that important”, “i go on it alot when im bored”)</td>
<td>106 55.2</td>
<td>104 58.4</td>
<td>182 63.0</td>
<td>116 63.4</td>
<td>508 60.3</td>
</tr>
<tr>
<td>Negative response (eg. &quot;not important&quot;)</td>
<td>10 5.2</td>
<td>10 5.6</td>
<td>22 7.6</td>
<td>11 6.0</td>
<td>53 6.3</td>
</tr>
</tbody>
</table>

*842 participants out of the 947 students who used SNS responded to this question.
Figure 18 illustrates that years 7 to 9 reported a decrease in the perceived importance of SNS. However, there was little change between years 9 and 10. This pattern needs to be investigated further since it is not reflected in the frequency of students updating SNS (see Figure 3), particularly in the significant increase in daily usage by year 10 students.

![Graph showing perceived importance of SNS by year.]

**Figure 18.** The importance of SNS to students.

**Why social networking sites are valued**

Students were asked to explain what they thought was the best thing about SNS. Table 23 reveals that almost half of the students who responded to this open ended question (n=432, 49% of 882 respondents) felt that the ability to stay in touch with friends and family was the best thing about SNS. A representative response was: “Being able to have a laugh with friends even when you are apart, see pictures of things that you did together and being able to vent.”

In addition to comments about communication with friends and family, 133 of the 432 students also commented that it was an added benefit that SNS, and especially the communication they afford, are free. The cost benefit was not just referring to the website service but also the fact that communication in any other method such as face to face or telephone are perceived to be more expensive. For example one student said the best thing about SNS was “catching up with people when you otherwise couldn’t or it cost you to instead.”

<table>
<thead>
<tr>
<th>Theme</th>
<th>Students (n=882)</th>
</tr>
</thead>
<tbody>
<tr>
<td>stay in touch with friends and family</td>
<td>432 49%</td>
</tr>
<tr>
<td>share similar interests with other people</td>
<td>35 4%</td>
</tr>
<tr>
<td>there is nothing positive about SNS</td>
<td>26 2.9%</td>
</tr>
<tr>
<td>Games or having fun</td>
<td>14 1.6%</td>
</tr>
<tr>
<td>anonymity</td>
<td>6 0.7%</td>
</tr>
<tr>
<td>Other (answers were either inappropriate or expressed lack of consideration such as “I don’t know”)</td>
<td>369 41.8%</td>
</tr>
</tbody>
</table>

Table 23

*The most valued aspect of SNS as reported by students*
In addition a smaller number of students (n=35, 4%) indicated that being able to share similar interests with other people was a benefit. This referred to not only sharing information within a social network such as “discovering new bands” but also SNS’ ability to expand students’ networks such as “their capacity to link you up with others with similar interests” and “their [sic] helpful when trying to promote yourself as a musician.”

A small number of students (n=6, 0.7%) felt that the best thing about SNS was the anonymity it offered. Examples of responses included: “you can put whatever you want on it,” “talking to people who don’t know what you really look like,” and “you can tell lies and no one knows it was you.”

Finally, only 26 students (2.9%) answered that there wasn’t anything positive about using SNS. A typical response was “i find them extremely boring.”

**The benefits of social networking sites**

Students were asked to identify the benefits of using SNS. This question returned very similar results to the previous question, with 442 students (48% of 921 respondents) seeing the main benefit to be staying in contact with their friends and family. However 30 students (3.3%) indicated that they thought it was a benefit to be able to expand their social network. For example, students explained: “Meeting and or getting to know more people. I got in touch with one of my role models and now we talk a lot which is great!” and “You get to meet new people and learn different things about others” and “GET MORE FRIENDS.”

Teachers were also asked to identify if there were benefits or advantages for students using SNS. The response was mostly positive with 127 teachers (62.3%) making favourable comments:

- 62 teachers (48.8%) suggesting that SNS are beneficial in “keeping in touch with people you don’t see regularly [and] rekindling friendships.”
- 25 teachers (19.7%) indicated that there were benefits to the school and for pedagogical activities including sharing resources between classes and to encourage collaboration.
- 40 teachers (31.5%) responded positively but did not elaborate.

In contrast 77 teachers (37.8%) indicated they felt there were no benefits for students using SNS. A representative response was: “They would be better off talking to each other and observing body language and able to have personal contact, a vital aspect of a balanced life.”

Parents were also asked to identify if there were benefits or advantages for their child when using SNS. Only 11 parents (22.4%) indicated that there were not aware of any benefits with some expressing a concern, for instance: “None as far as I am concerned. I would like it banned and have kids interact the old fashion way.” However the majority of parents (n=38, 77.6%) reported varying degrees of support for SNS from indifference (eg. “Some but not compelling reasons to encourage use of these sites”) to strong support (for example, “yes - finding people from old schools. finding people with similar interests. Having access to adult friends of the family who can exert influence. Having family on the site to interact. Being introduced to new ideas that are wonderful or to talents or art or videos” and “Numerous! Communication / learning / community / networking”).

[46]
4.7. Perceptions of risk

Students, teachers and parents were asked if they felt that students’ use of SNS included a degree of risk. It is perhaps not surprising that students felt that SNS were safer than their teachers and parents. Table 24 shows that while 48.8% of students recognised that there was some element of risk in using SNS over a quarter of students (28.3%) thought that SNS were safe. Perhaps just as worrying is that 19.6% of students were ambivalent by reporting that the degree of risk was not relevant because it is “just what everyone does”.

Table 24

<table>
<thead>
<tr>
<th>Level of risk</th>
<th>Students (n=906)</th>
<th>Teachers (n=204)</th>
<th>Parents (n=49)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>%</td>
<td>n</td>
</tr>
<tr>
<td>Fun and safe</td>
<td>256</td>
<td>28.3</td>
<td>9</td>
</tr>
<tr>
<td>Fun and a little bit risky</td>
<td>442</td>
<td>48.8</td>
<td>107</td>
</tr>
<tr>
<td>Very risky</td>
<td>30</td>
<td>3.3</td>
<td>35</td>
</tr>
<tr>
<td>Just what everyone does regardless of risk</td>
<td>178</td>
<td>19.6</td>
<td>53</td>
</tr>
</tbody>
</table>

In contrast with students’ responses, their teachers and parents were more cautious about the levels of risk associated with SNS use. Figure 19 helps to illustrate the difference between student and adult perceptions of risk. Teachers were particularly concerned that apart from students’ friendship networks, they were at risk of being contacted by undesirable people such as: “the occasional weirdo”, “anyone, creepy stalker types”, “I would imagine all sorts of people look at their sites, though, them being on the Internet and all. I doubt that those other people are social anthropologists, though, and i would imagine that their interest is largely prurient.”

Figure 19. Perceptions of SNS risk by students, teachers and parents.
However, not all students have the same perception of risk. Table 25 shows a comparison between each year level and is illustrated in Figure 20. While similar percentages of year 7 to 10 students feel that SNS are safe (approximately 25%) there is a decrease across the year levels in students perception of an element of risk with a corresponding increase in disregard for risk.

<table>
<thead>
<tr>
<th>Level of risk</th>
<th>Year 7 (n=213)</th>
<th>Year 8 (n=193)</th>
<th>Year 9 (n= 353)</th>
<th>Year 10 (n=147)</th>
<th>Total (n=906)#</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>%</td>
<td>n</td>
<td>%</td>
<td>n</td>
</tr>
<tr>
<td>Fun and safe</td>
<td>58</td>
<td>27.2</td>
<td>59</td>
<td>30.6</td>
<td>101</td>
</tr>
<tr>
<td>Fun and a little bit risky</td>
<td>121</td>
<td>56.8</td>
<td>96</td>
<td>49.7</td>
<td>167</td>
</tr>
<tr>
<td>Very risky</td>
<td>7</td>
<td>3.3</td>
<td>9</td>
<td>4.7</td>
<td>7</td>
</tr>
<tr>
<td>Just what everyone uses, regardless of risk</td>
<td>27</td>
<td>12.7</td>
<td>29</td>
<td>15.0</td>
<td>78</td>
</tr>
<tr>
<td>Total</td>
<td>213</td>
<td>100</td>
<td>193</td>
<td>100</td>
<td>353</td>
</tr>
</tbody>
</table>

*This table includes all student responses regardless of whether they use SNS. 98 students did not answer this question.*

When analysed according gender it is apparent that male and female students have similar perceptions SNS risk both within and across years (see Table 26). A small variation in this pattern which becomes apparent in Figure 21 is that slightly more (3.3%) male students reported that SNS were fun and safe in comparison with female students who were slightly more (3.6%) inclined to perceive them as fun and a little bit risky. While these differences are small, the same pattern is evident in each year level.
Table 26
Perceptions of degree of SNS risk by student year level and gender

<table>
<thead>
<tr>
<th>Students</th>
<th>Fun and safe</th>
<th>Fun and a little bit risky</th>
<th>Very risky</th>
<th>Just what everyone uses, regardless of risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>m (n=75)</td>
<td>n (%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Year 7</td>
<td></td>
<td>23 (30.7)</td>
<td>42 (56.5)</td>
<td>2 (2.7)</td>
</tr>
<tr>
<td></td>
<td>f (n=62)</td>
<td>16 (25.8)</td>
<td>35 (56.5)</td>
<td>2 (3.2)</td>
</tr>
<tr>
<td>Year 8</td>
<td></td>
<td>29 (31.2)</td>
<td>44 (47.3)</td>
<td>3 (3.2)</td>
</tr>
<tr>
<td></td>
<td>f (n=97)</td>
<td>28 (28.9)</td>
<td>49 (50.5)</td>
<td>5 (5.2)</td>
</tr>
<tr>
<td>Year 9</td>
<td></td>
<td>41 (29.3)</td>
<td>66 (47.1)</td>
<td>3 (2.1)</td>
</tr>
<tr>
<td></td>
<td>f (n=133)</td>
<td>35 (26.3)</td>
<td>67 (50.4)</td>
<td>2 (1.5)</td>
</tr>
<tr>
<td>Year 10</td>
<td></td>
<td>24 (26.4)</td>
<td>36 (39.6)</td>
<td>4 (4.4)</td>
</tr>
<tr>
<td></td>
<td>f (n=51)</td>
<td>10 (19.6)</td>
<td>23 (45.1)</td>
<td>2 (3.9)</td>
</tr>
<tr>
<td>Total</td>
<td>m (n=399)</td>
<td>117 (29.3)</td>
<td>188 (47.1)</td>
<td>12 (3.0)</td>
</tr>
<tr>
<td></td>
<td>f (n=343)</td>
<td>89 (26.0)</td>
<td>174 (50.7)</td>
<td>11 (3.2)</td>
</tr>
</tbody>
</table>

Figure 21. Comparison of male and female perceptions of degree of SNS risk.
Visibility of student SNS profiles

While students generally perceived their use of SNS to be safe or only a little bit risky, it is useful to contextualise this in terms of the degree of visibility of their SNS profile. As a general trend, students from years 7 to 10 are increasingly more selective in who can see their profile (see Table 27, illustrated in Figure 22). However, this means that year 7 students not only have more visible profiles and therefore be at greater risk but also are more likely to perceive SNS as safe or only a little bit risky (see Table 25) which in turn may generate complacency about risk aversion strategies.

Table 27
Reported visibility of student SNS profiles

<table>
<thead>
<tr>
<th></th>
<th>Year 7</th>
<th>Year 8</th>
<th>Year 9</th>
<th>Year 10</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(n=198)</td>
<td>(n=197)</td>
<td>(n=353)</td>
<td>(n=161)</td>
<td>(n=909)</td>
</tr>
<tr>
<td>n</td>
<td>%</td>
<td>%</td>
<td>%</td>
<td>%</td>
<td>%</td>
</tr>
<tr>
<td>Everyone (ie the whole world)</td>
<td>42 21.2</td>
<td>29 14.7</td>
<td>53 15.0</td>
<td>20 12.4</td>
<td>144 15.8</td>
</tr>
<tr>
<td>Everyone in my network (eg. school)</td>
<td>20 10.1</td>
<td>10 5.1</td>
<td>19 5.4</td>
<td>10 6.2</td>
<td>59 6.5</td>
</tr>
<tr>
<td>My friends and their friends</td>
<td>40 20.2</td>
<td>34 17.3</td>
<td>59 16.7</td>
<td>20 12.4</td>
<td>153 16.8</td>
</tr>
<tr>
<td>Only my friends</td>
<td>62 31.3</td>
<td>91 46.2</td>
<td>184 52.1</td>
<td>84 52.2</td>
<td>421 46.3</td>
</tr>
<tr>
<td>Only people I choose</td>
<td>34 17.2</td>
<td>33 16.7</td>
<td>38 10.8</td>
<td>27 16.8</td>
<td>132 14.6</td>
</tr>
<tr>
<td>Total</td>
<td>198 100</td>
<td>197 100</td>
<td>353 100</td>
<td>161 100</td>
<td>909 100</td>
</tr>
</tbody>
</table>

Figure 22. Visibility of student SNS profiles.

Parents were asked about their child’s SNS profile privacy settings. Most parents (n=33, 71.7%) believed their child’s profile could be viewed by friends or friends of friends while 11 parents (23.9%) indicated that they believed that ‘anyone’ or “Every man and his dog” could access their child’s profile. The remaining 2 parents were ‘unsure’ about the degree of accessibility of their child’s SNS. It is interesting to note that one parent suggested that the privacy settings were ineffectual, resulting in access for:
Those many individuals who’ve cracked the easy algorithms to access FB’s private info - including some paedophiles and some big companies looking to manipulate my son’s buying choices, and ASIO, and other government departments enabled to do so through the new ‘terrorised’ laws --- and probably others I haven’t considered, like insurance agencies.

**Perceived risks arising from student use of social networking sites**

In an open ended question, students were asked to explain if there were any risks or problems associated with the use of SNS. A total of 460 students answered this question (out of 1004 survey participants) and their responses are collated in Table 28. A small proportion reported that there were no risks or problems (14.9%) while others indicated that they had not considered the issue (6.8%). The implication is that 21.7% of students who answered this question were unaware or unconcerned about potential risks in using SNS.

<table>
<thead>
<tr>
<th>Risk or problem</th>
<th>n</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unwanted attention from others</td>
<td>147</td>
<td>31.9</td>
</tr>
<tr>
<td>Cyber-bullying</td>
<td>135</td>
<td>29.4</td>
</tr>
<tr>
<td>There are no risks or problems</td>
<td>68</td>
<td>14.9</td>
</tr>
<tr>
<td>Data security (eg. “hacking”, “identity theft”)</td>
<td>63</td>
<td>13.8</td>
</tr>
<tr>
<td>Had not considered the issue (eg. “don’t know,” “haven’t thought about it”)</td>
<td>31</td>
<td>6.8</td>
</tr>
<tr>
<td>Privacy issues (eg. “invasion of privacy,” disclosure)</td>
<td>15</td>
<td>3.2</td>
</tr>
<tr>
<td>Total</td>
<td>460</td>
<td>100</td>
</tr>
</tbody>
</table>

# 1004 students completed the surveys. This question was open ended and consequently a meaningful response could not be enforced. 544 surveys were not completed or included responses which did not answer the question. The remaining 460 responses were coded into the above categories.

Most of the students (61.3%) reported potential risks or problems from unwanted attention from others or cyber-bullying. Both of these concerns reflect the popular concerns of media and government. Students who reported the potential for unwanted attention from others (31.9%) made statements typical of:

- “if you add randoms then they could turn out to be weirdos”
- “creepy pedos [paedophiles] add you and try to get in your pants.”
- “It creates a haven for illicit paedophiles, stalkers etc.”
- “It brings undesirable people in closer reach and easier access”
- “randoms can add you and you have no idea who they are”
- “strange people contacting you”

In a separate survey question students were also asked if they had been contacted via their SNS in way that they did not like or found unpleasant. In response 637 students (72.4% of the 880 students who answered this question and who used SNS) responded that they had unwanted or unpleasant contact by strangers via their social networking profile. In contrast 243 students (27.6%) reported that they had not received such contact.
Returning to the consideration of Table 28 the students who identified cyber-bullying as a potential risk included examples of overt bullying such as “Sometimes people bully other kids, because it’s easier to say things over the internet, rather than to their face.” However the students also indicated issues of peer pressure, for example: “bullying, peer pressure, self esteem issues based on things like number of friends someone has or photos they have of a party that you weren’t invited to etc.”

![Risks or problems identified by students (n=460)](image)

**Figure 23.** Risks or problems associated with SNS identified by year 7 to 10 students.

A smaller group of students (n=63, 13.8%) identified security risks relating to their data such as people “hacking” into their SNS account or committing identity theft. For instance, one of the teachers reported:

> I have come across a student who showed me a site that was a mirror image of his own. And that person, whoever created it, tried to get his friends to add him on, pretending to be that person. So, yes, you do get imposters there.

However, the purpose of the identity theft was not known by the teacher or clarified by the students.

Another group of students (n=15, 3.2%) also identified a related issue of privacy, namely “invasion of privacy” and unwelcome disclosure of information about themselves by others. For instance one student in the interviews explained how students who do not have strict privacy settings can disclose information about themselves but also their friends, such as through the tagging (naming) of people in photos:

> Yeah, exactly. And so I have a friend, this really bugs me; I’m like get the picture off. She has all these pictures of her and her friends at school, and they’re wearing their uniform and everything. And she has random people, and it could be anyone. And she has all these photos, and she tags other people, other friends, and they’re like “Come on, can you please get that off?” And like they tag their friends.

Another student explicitly indicated they felt there was a risk of corporations gathering SNS profile and usage data for their own interests: “The fact that Google can track and monitor my
actions and build up a file on me from the actions on my Facebook page. Paedophiles etc. are the least of my worries, Google is watching me far more than them.”

Teachers and parents were also asked to identify any risks or problems which they perceived in their students/child use of SNS. The teachers were particularly concerned with issues of cyber-bullying (n=89, 43.6% of 204 teacher responses), for example: “harassment, taunts, make fun of others.” Another key concern was that of grooming or stalking (n=55, 27%), which one teacher described as “Huge risks regarding privacy and targeting by unwholesome sorts.” A third perceived risk was that of identity theft (n=29, 14.2%) by other students or strangers for a variety of reasons including malicious posting of false information, or the use of the identity for financial gain.

The parents, like the teachers, indicated that they were concerned with cyber-bullying (n=11, 22.4% of 49 parents) and grooming/stalking (n=6, 12.2%). One parent alluded that they were concerned about grooming but revealed that they were more concerned about what they felt was excessive screen-time:

I am aware that these sites can be misused by others, but we still are very careful about where he goes and who he goes with when he goes out - which he does very rarely. Main problem we have is that he spends far too much time on the site, particularly just waiting for others to respond. We are not good at managing this behaviour.

Another parent also pointed out that they felt their child was safe from unwanted contact but was susceptible to financial scams embedded in SNS. As with the previous parent, a key worry was in the management of the child’s behaviour:

My 'child' is not very trusting, so not many risks there any longer. The main risks come from his belief in the YOU Have Won MONEY pop-ups, and so on. If I let him have a credit card he would type in his info anywhere! He believes all the financial lying and finagling that goes on there. (He’s not reading this is he?) He thinks I am trying to get in the way of the clever-and-cutting-edge getting stuff-and-money schemes he 'finds' online. I do not know how to convince him they are all lying and stealing honey-foglers. What we used to call cons. He seems to think I’m just being mean to the nice online business community. I repeat: I HAVE NO IDEA HOW TO SAVE HIM FROM THIS.

Parents also reported risks to privacy in the form of disclosure (n=7, 14.3%), or as one parent said “giving too much info re themselves,” and was explained by another parent as “the public revelations of very private stuff. The mindset of the group where everyone is trying to be someone.” Four parents (8%) felt that there was little or no risk with statements such as “minimal, so long as there is parental supervision” or “Less risk than crossing a road.”

In an attempt to further clarify the risks for students when using SNS the research also conducted interviews with several experts in fields related to student use of SNS. Professor Jock Given, Professor of Media and Communications at the Institute for Social Research (ISR) at Swinburne University pointed out that “The use of Facebook makes the formation and conduct of relationships more transparent.” For instance, you know when couples “break up.” There is not as much privacy to relationships when it is all acted out for everyone to see in the status updates. Professor Given pointed out “the construction of self in the electronic environment can bleed into the real life environment” and consequently “privacy is an issue. Kids who have grown up in the public eye have to act out the identity they have chosen to represent through the social networking site... There may be less ability to change your mind about who you are. This is a huge challenge.”
Communication about risks between students, teachers and parents

The data has shown that most teachers and parents are aware of a variety of risks for their students/children. Similarly a large number of students identified a variety of risks associated with using SNS. However there is surprisingly little ongoing conversation between parents and their children and teachers and their students.

Almost half of the students (46.1%) reported they did not talk with their parents, and almost three quarters of the students (74.6%) reported that they did not talk with their teachers about their use of SNS (see Table 29). Some of the student responses indicated that they would like the opportunity to talk about it (eg. “No as they don’t let me.”) however the majority of students were strongly opposed to the idea, for example: “hell NO!” and “Noppe because i dont see the point it's none of there busniss.”

Table 29
The extent of students talking with parents and teachers about SNS

<table>
<thead>
<tr>
<th>Response</th>
<th>Do you talk to your parents/guardians about the use of social networking sites?</th>
<th>Do you talk to your teachers about the use of social networking sites?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>%</td>
</tr>
<tr>
<td>Yes</td>
<td>263</td>
<td>29.1</td>
</tr>
<tr>
<td>Yes, but infrequently</td>
<td>225</td>
<td>24.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>418</td>
<td>46.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>906</td>
<td>100</td>
</tr>
</tbody>
</table>

Many students indicated that they felt their teachers were not experienced enough to talk about the risks of using SNS. For instance one student said: “They ALWAYS lecture about stuff...when they don’t have a CLUE what they are talking about.” However, the same student supported his claim by explaining that cyber-bullying was just another form of bullying, and that he and his friends can easily protect themselves from unwanted contact by others. The self-assured nature of this and other students’ responses implies that students are clearly aware of some risks, but feel that those risks can be managed without adult help or advice.
However, the origins of their self-assurance was unclear. Presumably they learned the concepts and implications of cyber-bullying, online grooming and stalking, identity theft and risks to privacy from somewhere. The negotiation of meaning surrounding online risks and particularly those relating to SNS is a line of inquiry which should be pursued in future research to better understand how, why and when students develop, change and act on understandings of risk in the social web.

Although the majority of students (74.6%, Table 29) reported that they had not discussed SNS risks with their teachers, a similarly large proportion of teachers (68.6%, Table 30) reported that they had discussed SNS risks. The scope of the survey did not allow for the researchers to interrogate this discrepancy. It could be that the discussion offered by the teachers was not recognised as such because it was too brief, for instance 24.5% of teachers indicated that they only occasionally dealt with the issue with some teachers offering explanations that since the topic was not part of their curriculum they could ill afford to spend too much time on the issue. Indeed, 8.8% of teachers specifically stated that they did not talk about the issue because they thought it was covered by another teacher, usually in the students’ IT classes. However, not all of the teachers were certain in their knowledge: “I would think they would cover this in their IT classes.” This should also be contextualised by the fact that not all schools include compulsory IT classes and even if they did the curriculum for middle school students does not specify the topic of online risks in using SNS. Not only is it unclear where and how online safety education is dealt with within the curriculum, Cybersafety expert Robyn Treyvaud also noted that most schools have the wrong focus:

So for schools I think they’re focussing very much on policy leadership, filtering, you know all the technology stuff. I think it’s very much weighted to infrastructure and I don’t see a lot happening in terms of effective education in terms of the students, the teachers, parents and the wider community, and I see very few schools being very proactive about developing partnerships with the students in their schools to move forward in this very positive digital citizenship domain.

Clearly future research needs to be conducted with a view to understanding if, when and how schools can systematically raise awareness in students of risks associated with online activity, and especially in regard to SNS.
Table 30
*Teachers’ reports of discussing SNS risks with students*

<table>
<thead>
<tr>
<th>Response</th>
<th>n</th>
<th>%</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>90</td>
<td>44.1</td>
<td>“Yes... we show how to explicitly set Facebook security settings and why, ... learn about digital footprints, promote students to foster positive behaviour through these sites, promote student technology captains as a student voice for what they want to know about”</td>
</tr>
</tbody>
</table>
| Yes, sometimes or briefly | 50  | 24.5 | “not often enough”
“Sometimes. If I am trying to diffuse a situation which has been created because of social networking sites. But I am too busy trying to cover the curriculum most of the time!!” |
| No, it is covered by someone else | 18  | 8.8  | “Not personally, but I know they cover it in IT classes”
“No but I would think they would cover this in their IT classes”
“No, no need to as I don’t run an IT class or class related to these” |
| No       | 46  | 22.6 | “No, I am more interested in getting them back on task”
“only in so much as ‘get off that site now’” |
| Total    | 204 | 100  |                                                                                                                                          |

Teachers often commented on the lack of time in the curriculum for them to seriously address the issue of risks in using SNS.

Overall, the survey of 204 teachers indicated that 31.4% of teachers did not talk about the issue with their students and a further 24.5% only talked about it sometimes or briefly. In comparison, Table 31 presents data from the 49 parents who were surveyed, and reveals that only two parents (4.1%) had not talked about SNS risks with their child, with a further two parents (4.1%) had only talked about it sometimes or briefly. The vast majority of parents (n=45, 91.8%) reported, without equivocation, that they had talked with their children about the risks associated with using SNS. However, these results may be influenced by the fact that the parent surveys were conducted online, and was on a voluntary basis. Consequently the specific parents who self-selected to complete the survey may have already had some interest in the issue.
Table 31
*Parents’ reports of discussing SNS risks with their child*

<table>
<thead>
<tr>
<th>Response</th>
<th>n</th>
<th>%</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>45</td>
<td>91.8</td>
<td>“oh yes yes yes yes yes yes”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“Yes, discuss quite often risks of allowing too much info on site”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“Yes, We are constantly reminding her”</td>
</tr>
<tr>
<td>Yes, sometimes or briefly</td>
<td>2</td>
<td>4.1</td>
<td>“only very briefly”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“Yes a while ago, but need to do it again.”</td>
</tr>
<tr>
<td>No</td>
<td>2</td>
<td>4.1</td>
<td>One of the two parents simply stated “no” while the other explained that</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>their child does not use a SNS implying that this means they do not</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>need to discussing potential risks with their child.</td>
</tr>
<tr>
<td>Total</td>
<td>49</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

Even though a large proportion of parents had reported that they talked to their child, many of them indicated that their child displayed some reticence to listen:

- “Yes, a little...she is reluctant to talk too much about it saying there are no problems and nothing to worry about”
- “yes, but it is mostly dismissed unless another peer who is respected agrees and advises to tighten up or be more secure”
- “Yes, often. Have discussed with her that I do not want her known as the "Corey Worthington" of our suburb, to which she replies "I know, & how stupid do you think I am!!"”
- “Constantly, but the peer opinion about it counts much much more. It feels private and fun and harmless to the kids when using it, though they can spout all the dangers when thinking about it while disconnected from it.”

This last quote suggests that there is a disconnect between the espoused wisdom and enacted behaviour of children. Further research should be conducted to correlate students’ knowledge of risks and risk aversion strategies and their online behaviour.

**Students’ risk aversion strategies**

The majority of students (72.4%, Table 32) had reported that a stranger had contacted them via SNS which was either unwelcome or unpleasant. These students were then asked what they did in response to that contact. The answers were then coded according to themes arising from the data. Despite 514 students reporting their strategies they could all be coded according to two types of strategies. Table 32 shows that 43.4% of the students reported that they had deleted (21.9%) or blocked (21.5%) the unwelcome contact. A further 15% of the students reported that they ignored the contact. The remaining 14% of students did not explain if or what strategy they employed. The strategies employed by the students are reasonable, however it is noteworthy that none of the students reported that they told an adult, notified the SNS company of an inappropriate contact, or reviewed their own security settings.
Table 32
Strategies in response to unwelcome contact via SNS

<table>
<thead>
<tr>
<th>Response category</th>
<th>n</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>deleted or blocked the unwelcome contact</td>
<td>382</td>
<td>43.4</td>
</tr>
<tr>
<td>ignored the contact</td>
<td>132</td>
<td>15.0</td>
</tr>
<tr>
<td>no action was specified</td>
<td>123</td>
<td>14.0</td>
</tr>
<tr>
<td>No n/a</td>
<td>243</td>
<td>27.6</td>
</tr>
<tr>
<td>Total</td>
<td>880</td>
<td>100</td>
</tr>
</tbody>
</table>

*of the 957 students who reported using a SNS, 880 students answered this open ended question. The responses were coded according to themes arising from the data.*

In a separate survey question the students were asked to explain the strategies they knew of to avoid any risks or problems associated with using SNS. The students identified 9 strategies they used to avoid risks or problems (see Table 33). Only 4.2% of the students reported that they were unaware of strategies.

Table 33
Students’ reported strategies for avoiding SNS risks or problems

<table>
<thead>
<tr>
<th>Strategies for avoiding risks or problems associated with SNS</th>
<th>n</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. did not accept “friendship” requests of people they did not know, or ignored the unwanted approaches</td>
<td>225</td>
<td>24</td>
</tr>
<tr>
<td>2. “blocking” or “deleting” unpleasant or unwanted “friends”</td>
<td>141</td>
<td>15.0</td>
</tr>
<tr>
<td>3. setting their profile to “private”</td>
<td>95</td>
<td>10.1</td>
</tr>
<tr>
<td>4. not disclosing personal details</td>
<td>86</td>
<td>9.1</td>
</tr>
<tr>
<td>5. frequently changing their password</td>
<td>27</td>
<td>2.9</td>
</tr>
<tr>
<td>6. threatening people who wished to be added to the student’s SNS</td>
<td>12</td>
<td>1.3</td>
</tr>
<tr>
<td>7. self censorship, e.g., ‘being careful about what you say’,</td>
<td>54</td>
<td>5.8</td>
</tr>
<tr>
<td>8. unspecific ‘motherhood’ statements e.g. be safe, be sensible, don’t do bad things on it</td>
<td>38</td>
<td>4.1</td>
</tr>
<tr>
<td>9. Talk to teachers or parents</td>
<td>9</td>
<td>1.0</td>
</tr>
<tr>
<td>did not know of any strategies</td>
<td>39</td>
<td>4.2</td>
</tr>
<tr>
<td>did not answer the question, e.g. “never had a problem,” or provided nonsensical or inappropriate answers</td>
<td>212</td>
<td>22.5</td>
</tr>
<tr>
<td>Total</td>
<td>938</td>
<td>100</td>
</tr>
</tbody>
</table>

*938 students responded to this question.*

Most of the students conveyed the sense that strategies in dealing with risks associated with SNS are common sense. For instance, one student said: “Um, don’t post shit that can get you in trouble? Duh!” Another student explained:

if we get added by some random person we have never heard of, we dont talk to them :|
its actually pretty easy to tell if a profile is real or fake anyway. No one i know has ever
been lured into a trap by some pedo or something and told anyone they didn’t know
where they lived or whatever. We don’t stand in the middle of the street yelling "I LIVE ...."
do we? I barely even give my friends personal information (mobile no. etc) over the internet, just in case (most people are the same).

This was similar to most of the responses and is even more succinctly described by one students as: “If they sound sus, don’t contact them anymore. If they ask for details like an e-mail address, etc. ignore them eternally. If they sound too innocent, take them for a freak. xD” However, while the students expressed a confidence in their ability to recognise a “fake,” “freak” or someone who is “sus” they do not elaborate how this is achieved.

The same strategies and the implied message that such strategies are common sense were also found in the student focus group interviews. In one interview students explained that they can protect themselves from cyber-bullying by taking similar precautions to those they already know from outside of online spaces, and in this case, being careful to not escalate situations by removing themselves from the situation:

**Student A:** Yeah, I was just going to say the same thing. Like bite your tongue, and really - because I’ve made a few mistakes in the past. Like someone has been mean to my friend, and I’ve got involved, and like you’ve said things. Like don’t get involved, and just if someone is being really mean, don’t defend yourself. Like yeah, if it’s really bad, defend yourself, but don’t be mean, because you’re being the exact same as them. Don’t get involved. Try not to get involved and just block them or something.

**Student B:** Like in real life sometimes there are fights at a train station, and this one person is getting really aggressive towards someone else, and that other person just walks away. You could do that on a chat site as well. Like what Student A was saying, just block them, forgive and don’t forget sort of thing.

**Interviewer:** Forgive and don’t forget?

**Student B:** Yeah. Not forgive and forget, because if you forget it could happen again.

The strategy of “forgive and don’t forget” may be useful in learning to identify and extricate oneself from situations which may escalate. However, only 9 students (1%) in the surveys and none in the interviews suggested that they would ask for the guidance or help of adults. It has already been pointed out that the self-assured nature of all of the students with regards to their safety in using SNS is a characteristic which needs to be researched further.

Through the interviews the strategies of students were further interrogated. A number of the students indicated that they protected their privacy by not providing all or accurate information online. Using a pseudonym or nickname is an obvious strategy but which only one student mentioned:

**Student C:** On Fan Fiction we have a profile page, and you put up you, and I’ve put up my name, but I haven’t put up all my name, my proper name. I’ve just put up sort of a nickname.

**Interviewer:** So you’re protecting your identity in that way?

**Student C:** I’m sort of twisting the truth, just a little white lie to protect myself.

Another student explained how she manipulated her profile information to protect herself from unwanted contact:
Not many people really go onto other people’s profiles to see when their birthdays are or whatever. You can make them fake, but not everything has to be fake. You can still have your name so that your friends know who you are and can add you as a friend or whatever if you’re new. But my profile, for example says that I’m 18, because yeah, I didn’t want to put my real age unless there might have been some creep...

It surprised the researchers at the time that students might pretend to be older as a risk aversion strategy. Nevertheless, while the decision to provide an older age in her SNS profile was a purposeful risk aversion strategy (presumably to protect herself from paedophiles), it may also afford other risks.

4.8. Teachers’ use of SNS

During the course of this research two issues became increasingly of interest with regards to teacher’s use of SNS. Firstly, in what ways do teachers use SNS for educational purposes and what are the risks involved in such activity. Secondly, how does the increased access and profiling afforded by SNS affect teachers’ lives and in particular, can lead to risk. Since this line of inquiry arose during the project the researchers decided to add the questions even though 115 teachers had already completed the surveys. Consequently, the final 89 of 204 teachers were asked if they used SNS and the degree of visibility of their SNS profile.

In response, 61 teachers (68.5% of the 89 teachers, see Table 34) reported that they did use a SNS. 23 teachers (37.7% of 51 teachers who used SNS) had relatively low privacy settings (for example, everyone or friends of friends could see their profile). However, 62.3% were selective about who could access their SNS profile. One of the teachers in the interviews tried to explain his reasoning for being selective:

Yes. I have my own Facebook site and use it to keep in touch with friends on holidays overseas etc and it is great to be able to see their photos and share in their experiences. But I do not have any ‘friends’ who are not actually friends!! As an adult I have a very different perspective to my students as to how and what I use the site for. I feel relatively safe in the way I use my site, I think it is rather risky the way the students use their sites.

Table 34
Visibility of teachers’ SNS profiles

<table>
<thead>
<tr>
<th>Do you use SNS</th>
<th>n</th>
<th>%</th>
<th>Visibility</th>
<th>n</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>61</td>
<td>68.5</td>
<td>Everyone (ie the whole world)</td>
<td>11</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Everyone in my network</td>
<td>7</td>
<td>11.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>My friends and their friends</td>
<td>5</td>
<td>8.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Only my friends or people I choose</td>
<td>38</td>
<td>62.3</td>
</tr>
<tr>
<td>No</td>
<td>28</td>
<td>31.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>89</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The teachers who reported having a SNS were then asked if they had used SNS in an educational context. 63.9% (n=39) of the teachers reported that they had not used SNS in an educational context. Although two of the teachers had indicated that while they have not used
it in an educational context they used SNS to keep in contact with ex-students. A more common response to the question is exemplified in this quote:

the students talk about social networking sites during school time in their personal conversations. I do not speak about it on a personal level although students will ask if I have Facebook. I decline to comment as I feel that it is not appropriate to discuss the personal nature of Facebook with students.

However 36.1% (n=22) of teachers who used SNS indicated that they had used SNS for educational purposes. Two of the teachers indicated that they used SNS to collaborate with colleagues, for example: “To send UK friends who are teachers clips or links I have used in Aus.” The remaining 20 teachers reported that they had used SNS with their students, for example:

- “yes i have used sns for educational contexts...when working on creating a video, sharing information, discussing info”
- “yeah to tell students about dates they should know, reminders, and to put up links to must see sites”
- “Yes. To pass on information to my Year 12 students when I have been absent.”
- “yes- made group for year 12 students for info/collaboration”
- “yes, as a invite only site for resources”
- “yes, to send message to students about marks or work”
- “yeah to organise a holiday practice exam – EVENT”

This is corroborated by several comments from students, such as: “i talk to my teachers on Facebook, its helpful if i need help with homework or whatever.” Commenting on the use of SNS in education, Cybersafety expert Robyn Treyvaud stated that “it’s got to the point where it’s not negotiable.” In Ms Treyvaud’s opinion SNS need to be used in day to day teaching practices, and proposed a litmus test: “Are we preparing children for our yesterday or for their tomorrow? To me it’s a no brainer.” However, she also points out that the effective use of SNS by teachers with students is inhibited by many teachers’ limited understanding of the media, let alone the pedagogical consequences of the media, including shared content creation. In addition to misunderstanding by teachers, Ms Treyvaud pointed out that schools are “not really clear about security, privacy, protection, duty of care because these sorts of things haven’t a. been discussed and b. they aren’t necessarily documented.”

All of the teachers were also asked to identify any risks, especially legal risks, for teachers using SNS. Only 16 teachers (7.8%) said that they were not aware of or were unsure about any legal risks for teachers using SNS. Only one of these teachers indicated apathy in this regard: “dunno don’t care.” In addition to the teachers who were not aware or unsure there were an additional 20 teachers (9.8%) who expressed concern about risks but their answers did not specify what those risks were, for example “enormous risks.” The remaining 168 teachers (82.4%) expressed a range of concerns related to libel, disclosure and privacy. None of the teachers suggested risks of breaching copyright, intellectual property or criminal law.

A common theme of concern, expressed by 166 teachers (81.3%), was that due to the informality of SNS and the potential to share too much information in either direction that it risks compromising their professionalism, ability to teach and in some cases resulting in issues related to their duty of care.

56 teachers (27.5%) made non-specific statements about risks in relation to duty of care. However 61 teachers (29.9%) clearly identified concern that there may be legal issues for
teachers due to inappropriate information being discovered by teachers on students’ profiles which may create a professional or legal obligation to act. For instance:

- “Problems with knowing what your students are doing, drinking, smoking etc on weekends”
- “Potential knowing information about students and their activities and having a legal obligation to report on these issues.”

An additional 49 teachers (24.1%) were concerned about the implications of students finding out information about the teacher which not only constitutes “privacy loss” but could negatively impact on the professional relationship between the teacher and student with the implication that it will impact on the teacher’s ability to teach, for example:

- “Students accessing personal information which is inappropriate or alters their perception of teachers”
- “I think it is risky for teachers to be ‘friends’ with students. It blurs the line between your professional and personal life.”
- “Maybe for younger staff members it could involve some break down of necessary teacher / student barriers.”

The teachers also pointed out that the disclosure of information through SNS may not only put their professional role at jeopardy but also it can be used maliciously by students, for example: “potential for students to gain information about a teacher and use it inappropriately.”

Two teachers in the interviews indicated that they believed using SNS with students was “illegal,” and another teacher responded in the survey that “[SNS use] does not adhere to DEECD Duty of Care Guidelines.” However, at the time of writing, these teachers were incorrect. This research did not have the opportunity to further interrogate the validity of teachers’ perceptions of risk. While many expressed a concern regarding their duty of care being compromised, it may be useful in future research to more closely investigate the risks perceived by teachers and validate their relationship to legal concerns (such as duty of care), professional regulatory body requirements such as code of conduct and the educational institutions’ requirements.

It is interesting to note that two of the teachers highlighted that a risk of SNS was not sharing of information between the teacher and student, but instead arose from the potential for students to see or connect with “friends” of the teacher and for the teacher to see or connect “friends” of the students. One of the teachers reported, “My husband has been contacted by ex students of mine,” which resulted in her not using SNS. Another teacher pointed out that he cannot control the content posted by his friends: “I don’t know what my friends are going to write. My friends can write some pretty offensive things.” As a result this teacher has two SNS, one for his personal use and the other strictly limited to his students.

4.9. **Summary**

The results indicate that there is a degree of awareness of risks in using SNS by middle school students, although concerns about risks differ markedly between parents and teachers, on the one hand, and students, on the other. The research findings also indicate that there is a high degree of trial and error in how middle school students are seeking to manage risks associated with SNS use. Moreover, although there is some degree of understanding of legal risks, there is very little clear understanding by students, parents and teachers alike, of the precise nature of
the legal risks that may arise from everyday SNS use. On the other hand, there is much more awareness of the more dramatic consequences of cyber-bullying. While there is some awareness of the social context within which use of SNS takes place and some attempt to moderate behaviour accordingly, such as by teachers not ‘friending’ their current students, there seems to be very little awareness of the legal context within which SNS use occurs. Users do not read the terms of the user agreement which in fact regulates their use of the service and may prohibit much of the risky conduct in which they are engaged.

This leads to the question of how useful terms of agreement may be in regulating behaviour, and further questions regarding the role of the agreement in alerting users to risks? Also, how many of these risks are created by the agreement itself? The next section will consider the standard terms of user agreements applicable to the most commonly used SNS.
5. The legal risks faced by young people using SNS

This chapter provides a description and analysis of the legal risks facing children and young people in the use of SNS, which were introduced in chapter 2. In doing so, the chapter first explains the Terms of Service (ToS) which govern the use of SNS. The chapter then explains the main areas of legal risk identified by the project, including potential infringements of intellectual property rights (IPRs), breaches of privacy and disclosure of personal information, defamation and potential liability for cybercrimes. The chapter proceeds to explain the issues relating to legal capacity and liability of children and young people. Finally, the chapter illustrates the potential legal risks by explaining the legal issues that arose when a Melbourne teenager posted explicit photographs of Australian Rules football players to her Facebook site in late 2010.

5.1. Terms of Service

The use of all SNS is governed by their contractual terms, which go under a variety of names, but which are commonly called Terms of Service (‘ToS’). Under Australian law, click-through agreements, such as the ToS of SNS, are likely to be considered binding on adults. The extent to which such agreements are binding on minors is considered further below at section 3 of this chapter.

In order to understand the obligations imposed upon users, and in order to ascertain if there were any major differences between the ToS adopted by the providers, the research team conducted a comprehensive review of the ToS of the key SNS, as indicated by the responses to the survey instrument. These were:

- Bebo
- Tumblr
- Twitter
- MySpace
- Facebook

The ToS of YouTube and MSN were also considered, as these services were mentioned frequently by students in their survey and interview responses, even though they are not, strictly speaking, SNS. In particular, a lot of students linked material from YouTube to their SNS profile.

As expected, there was a high degree of similarity in the majority of the ToS contained in these agreements, even though the terms are slightly differently worded for the different services. Therefore, the following overview provides some generalised comments with examples of the key terms. Any major differences between the various providers are then identified.

It should be noted at the outset that, although SNS are often perceived by their users as a ‘community space’ or ‘social space’ facilitating interaction between users, the contractual relationship exists only between each end user and the service provider. There may be rules of conduct that regulate behaviour between users, such as community guidelines, but there is no contract between the users themselves. Consequently, in the event of a dispute, the end user
can only seek to enforce any ToS through the action of the service provider. If the service provider chooses not to intervene in a dispute between users, which is usually the case, users are left with little recourse.

This contractual model reflects the nature of user-generated content (‘UGC’) sites generally – including YouTube, Twitter and Flickr - where users post content which is not moderated or filtered prior to it being made publicly accessible. This business model saves the provider both time and money, as well as facilitating rapid posting and ‘sharing’ of content. Many of the ToS reflect this business model.

ToS presented on a ‘take it or leave it’ basis

Each of the agreements reviewed for this project is presented on a ‘take it or leave it’ basis, with users being deemed to consent to the terms by means of using – or, in the case of changes, continuing to use - the services. The means for providing users with notice of updates or changes to the ToS vary slightly from service to service, with some offering to provide email notice of changes and others merely warning users to regularly check back to the page that sets out the ToS.

Example:

MySpace reserves the right to modify this Agreement at any time and from time to time, and each such modification shall be effective upon posting on the MySpace Services. All material modifications will apply prospectively only. Your continued use of the MySpace Services following any such modification constitutes your agreement to be bound by and your acceptance of the Agreement as so modified. It is therefore important that you review this Agreement regularly. If you do not agree to be bound by this Agreement and to abide by all Applicable Law, you must discontinue use of the MySpace Services immediately. You may receive a copy of this Agreement by contacting us at our Help site.

MySpace Terms of Agreement, as at 27 September 2010, http://www.myspace.com/Help/Terms

Of course, the majority of users of SNS, including adults and minors, do not ever read the ToS, so few users are even aware of the conditions imposed upon them, although they are bound by them. For example, the following exchange occurred in one of our interviews:

Interviewer: ... So you don’t even remember seeing those sort of things from Facebook come up?
Student 1: No, I just click yes.
Interviewer: So it probably came up?
Student 1: Yeah probably, but nobody reads them.

Complexity of drafting and language

The ToS for each of the SNS reviewed for this project adopts a different tone and level of reader complexity. The Twitter ToS are drafted in plain English and are the most user-friendly in terms of explanation of terms used, even including ‘tips’ that elaborate on the point being made. Despite the use of plain English and ‘tips’ being regarded as best practice, the ToS of other services are drafted in more complex ‘legalese’.

[65]
Age limitations

There are important differences in the age limitations imposed by the ToS of SNS reviewed for this study. While some agreements, such as the ToS for Twitter, refer to the need for users to be of an age where they can form a binding contract, the others, including Bebo, Tumblr, MySpace and Facebook, specify a minimum age of 13 years. The thirteen years age limitation derives from the US Children’s Online Privacy Protection Act of 1998 (US) (COPPA), which regulates the collection of private information from a person under the age of 13.

In addition to the general age restriction, the ToS for MySpace include a term which allows them to delete the profile of any user whom they believe to be under 18 and who represents themselves as 18+, or any user whom they believe to be over 18 who represents themselves as under 18 years of age. Facebook also reserves the right to ‘add special protections for minors (such as to provide them with an age-appropriate experience) and place restrictions on the ability of adults to share and connect with minors, recognizing this may provide minors a more limited experience on Facebook.’

Applicable law

All of the ToS reviewed for this project purport to be subject to US laws, except for the Microsoft agreement, which presents a range of options for international users. In each case the user is required also to comply with any domestic laws that may apply to them, without specifying what these may be. This, of course, presents a major challenge for the average user, who would have no idea of the range of laws that may apply to their use of the service.

Disclaimer of liability

All of the ToS reviewed for this project include a disclaimer exempting the service provider from responsibility for any Content that is posted on or distributed by the Service.

Example:
You are solely responsible for your conduct and any data, text, information, graphics, photos, profiles, audio and video clips, links and other content ('Materials') that you submit, post and display on the Bebo Service.

Bebo Terms of Use, as at 12 September 2010, http://www.bebo.com/TermsOfUse2.jsp

In addition, all of the ToS incorporate a general disclaimer of liability for all and any loss or damage arising from use of the service. Tumblr, however, includes a specific disclaimer in respect of its ‘Meetups’ service, which offers a platform for arranging face-to-face meetings at ‘restaurants, bars and other venues all over the world.’ The Tumblr disclaimer is obviously designed to address the particular risks that may be associated with face-to-face meetings.

Example:
To the fullest extent permitted under applicable law, Tumblr disclaims all liability, regardless of the form of action, for the acts or omissions of other Tumblr users or any other third party and will not be liable for any damages, direct, indirect, incidental and/or consequential arising out of your organization or attendance at a Meetup or your interactions with any Tumblr user or third party you meet at such events.

Tumblr Terms of Service, as at 27 September 2010, http://www.tumblr.com/terms_of_service
Monitoring and removal of content

The interviews with students conducted for this project indicated that the majority of content posted to SNS was what the users identified as ‘user generated’. Despite this, it was clear that much of this was material that the students had found on the internet, then saved to their own computer, before posting it to their profile. These practices fit within the business model of content aggregators, such as YouTube and SNS providers, which is generally to encourage users to post content without any monitoring or filtering by the service provider, but with the service provider removing content in the event of a complaint or threat of legal action.

The ToS for each of the SNS reviewed for this project disclaim any obligations to monitor content. Nevertheless, while each service provider retains an absolute discretion to remove user content, the ToS incorporate slightly different rules about the circumstances in which content may be removed.

Example:

We may, but shall have no obligation to remove or limit access to Materials originating from any Bebo user that we determine in our sole discretion are unlawful, fraudulent, threatening, libellous, defamatory, obscene or otherwise objectionable, or infringes or violates any party’s intellectual property or other proprietary rights or these Terms of Service. Further, under no circumstances does Bebo have any obligation to check the accuracy or truthfulness of any Materials, not to monitor any Member’s use of the Bebo Service.

Bebo Terms of Use, as at 27 September 2010, http://www.bebo.com/TermsOfUse2.jsp

Facebook contains a unique provision, dealing specifically with ‘memorialising accounts’. This provides that if Facebook are notified that a user is deceased, the user’s account may be memorialised, thereby restricting access to confirmed friends and allowing ‘friends and family to write on the user’s Wall in remembrance’. The account will be closed upon formal request from the user’s next of kin or other proper legal request.

With respect to material which users want removed from their page, or the closure of accounts, the ToS for most of the sites provide a warning that material may remain accessible post-removal or post-termination.

Example:

On termination of Subscriber’s membership of the Site and use of the Services, Tumblr shall make all reasonable efforts to promptly remove from the Site and cease use of the Subscriber Content; however, Subscriber recognizes and agrees that caching of or references to the Subscriber Content may not be immediately removed.

Tumblr Terms of Service, as at 27 September 2010, http://www.tumblr.com/terms_of_service

Protection of user name and password

The ToS for all services provide that the user must retain their user name and password in private, and not share the details with any other person for any reason.

Example:

You are entirely responsible for maintaining the confidentiality of your password. You agree not to use the account, username, email address or password for another Member at any time or to disclose your password to any third party. You agree to
notify MySpace immediately if you suspect any unauthorized use of your account or access to your password. You are solely responsible for any and all use of your account.

MySpace, as at 27 September 2010, http://www.myspace.com/Help/Terms

This provision, which many young users may not be aware of, reinforces the importance of users taking care to manage their own identity information.

**Acceptable user names**

Rules relating to the selection and registration of a user name included in the ToS of SNS relate largely to prohibitions on impersonation of third parties. There are also prohibitions upon transferring or selling accounts. As explained below, these terms are supplemented, under Australian law, by criminal offences relating to identity theft.

**Prohibited conduct**

The ToS of each service reviewed for this project also include a list of prohibited user conduct. The prohibited conduct generally encompassing the following:

- Content which is offensive, or which incites or promotes racism, hate, bigotry or physical harm against any group or individual;
- Harassment or the encouragement of harassment of another person;
- Content which is sexually explicit, excessively violent or which exploits violence or sexual violence, contains nudity or links to an adult website or adult content (in some cases, subject to the limitation that there may be a link if sufficient warning is given);
- Content which promotes or facilitates illegal conduct or behaviour;
- Content which defames, abuses, stalks, threatens or otherwise violates the rights of other people;
- False and misleading materials, including a false or misleading identity;
- Viruses, Trojan horses, worms, or any other malicious code;
- Spam and other unauthorised advertising material, including pyramid schemes and chain letters;
- Programs to harvest email addresses or solicit or collect personal information;
- Material belonging to third parties;
- Material disclosing the personal information of other people;
- Any programs or content which may place an undue burden on the service.

The importance of the comprehensive lists of prohibited conduct is essentially twofold: it provides some protection for SNS providers against liability for the unlawful behaviour of users, but also confers considerable discretion on SNS providers over the suspension or cancellation of user accounts.
**Intellectual property rights (IPRs)**

The ToS for all services require users to warrant that the material that they upload to SNS does not infringe the IPRs of third parties. Moreover, each SNS reviewed for this project has a notice and take-down procedure which complies with the US copyright ‘safe harbour’ regime. The ‘safe harbour’ regime, established under the US Copyright Act and effectively incorporated into Australian copyright law, limits the liability of service providers that host infringing content, provided they establish a system for the notification and removal of allegedly infringing material.

In addition, the ToS for several of the Services reviewed for this project provide for termination of a user’s account in the event of multiple copyright infringements.

*Example:*

You may not post, modify, distribute, or reproduce in any way any copyright material, trademarks, or other proprietary information belonging to others without obtaining the prior written consent of the owner of such proprietary rights. Bebo respects the intellectual property rights of others and reserves the right to terminate any user’s access to the Bebo Service according to these terms of use if Bebo is notified that such user’s activities infringe the rights of third parties on more than one occasion.

Bebo Terms of Use, as at 27 September 2010, [http://www.bebo.com/TermsOfUse2.jsp](http://www.bebo.com/TermsOfUse2.jsp)

Importantly, the ToS for the SNS also include a range of licences relating to user-generated content. In general, the ToS require users to grant a non-exclusive, worldwide, royalty free licence to use, distribute (and frequently modify, adapt and to create derivative works using) the content, with further rights to grant sub-licences and to transfer such rights to third parties. Some of these licences confer rights on the service provider only insofar as they are necessary to provide the SNS services, whereas others are not so confined.

*Example:*

Subscriber shall own all Subscriber Content that the Subscriber contributes to the Site, but hereby grants and agrees to grant Tumblr a non-exclusive, worldwide, royalty-free, transferable right and license (with the right to sublicense), to use, copy, cache, publish, display, distribute, modify, create derivative works and store such Subscriber Content and to allow others to do so (“Content License”) in order to provide the Services.

Tumblr Terms of Service, as at 27 September 2010, [http://www.tumblr.com/terms_of_service](http://www.tumblr.com/terms_of_service)

The Tumblr licence should be compared to the broader licence created in favour of Twitter, which allows rights of third party licensing and adaptation, whilst the User retains all liability for any use of the content by Twitter or any third party. That is, whilst the ToS for Twitter state that the User retains rights to the content that they submit, the User grants Twitter ‘a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed).’ The Twitter ToS then provide that the User is responsible for use of the Services, for Content they provide and ‘any consequences thereof, including the use of your Content by other users and our third party partners. You understand that your Content may be rebroadcasted (sic) by our partners and if you do not have the right to submit Content for such use, it may subject you to liability.’
Twitter will not be responsible or liable for any use of your Content by Twitter in accordance with these Terms. You represent and warrant that you have all the rights, power and authority necessary to grant the rights granted herein to any Content that you submit.

**Privacy policies**

The ToS for all the SNS reviewed for this project include a privacy policy, or link to a separate privacy policy. These policies provide information regarding the type of information being collected by the SNS, how that information is collected, what that information may be used for, and how it will be stored and processed. The policies also identify who that information may be shared with, such as third party advertisers or third party applications. In some cases, if the user opts not to disclose some personal information, some aspects of the service may not be available to them. Where personal information is used by a party other than the service provider, further use of the information may be governed by the privacy policy of the third party.

*Example:*

You may, of course, decline to submit personal information through YouTube, in which case you can still view videos and explore YouTube, but YouTube may not be able to provide certain services to you. Some advanced YouTube features may use other Google services such as Google Checkout or AdSense. The privacy notices of those services govern the use of your personal information associated with them.

YouTube, Terms of Service, as at 27 September 2010, [http://www.youtube.com/t/terms](http://www.youtube.com/t/terms)

The Facebook privacy policy is the most comprehensive of those reviewed for this project. This is unsurprising, given the controversy that has been associated with the Facebook privacy policy. The Facebook policy includes detailed descriptions of the operation of the Service’s privacy settings. Like the policies of many of the other Services, it also includes a discussion of the operation of cookies and why they need to be enabled to use certain aspects of the service.

The Facebook ToS also include the following warning or disclaimer (as well as links to a number of pages and resources for further help): ‘Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook. You can reduce these risks by using common sense security practices such as choosing a string password, using different passwords for different services, and using up to date antivirus software.’

**Summary**

Many users of SNS agree to the ToS of a SNS, which are presented as click-through agreements, without bothering to read or understand the terms. Nevertheless, the ToS establish the most comprehensive, and arguably the most important, legal rules regulating the use of SNS. Understandably, the ToS are drafted primarily to support the business model adopted by SNS providers, which is essentially to promote UGC. In broad terms, the ToS therefore seek to limit the liability of the SNS provider for content – including liability for
infringements of IPRs and for the personal information of users – while shifting responsibility to the users.

Given the importance that SNS, such as Facebook, have assumed in the social lives of users, and especially young users, the consequences of breaches of the ToS, which may result in suspension or cancellation of the user’s account, may be quite significant. An inability to access a SNS would effectively cut a person off from an activity that has become highly integrated into the lives of many young Australians. It is therefore important for young users to become familiar with the rights and obligations established by the ToS of SNS. This would also assist in promoting a broader understanding of the importance of understanding the consequences of entering into online contracts.

5.2. Legal risks of using SNS

This section of the chapter explains the relevant areas of Australian law relating to the risks of using SNS:

Privacy

Privacy is recognised internationally as a fundamental human right. Despite this, it is not easy to explain what is meant by privacy, because it can mean different things to different people. One of the best ways of explaining privacy, which has been accepted by the Australian Law Reform Commission (ALRC), is to divide it into the following four related concepts:

- **Information privacy**, which is about protecting your personal information, such as your medical records or credit history, when it is collected or used by government or business.
- **Bodily privacy**, which is about protecting your body against things like drug testing or physical searches, without your agreement.
- **Privacy of communications**, which concerns the security and privacy of telephone calls, email messages and other forms of communication.
- **Territorial privacy**, which is about setting limits on intrusions into your personal space, including video surveillance and ID checks.

Privacy is considered important because it can protect an individual’s freedom to make decisions for themselves. Privacy protection can also prevent other people from using information about an individual, without agreement, in ways that might harm or embarrass the person. For example, if someone uses a mobile phone to take a photo of a person doing something potentially embarrassing, then posts it to Facebook, this may affect the person’s reputation, and also how other people treat them.

It is generally accepted that society has a special obligation to protect the privacy of children. As the submission of the Office of the Privacy Commissioner to the cyber-safety committee inquiry explained:

Children are particularly vulnerable due to their limited capacity to make decisions about their own information and their reliance on others to ensure that their interests and rights are protected. The potential consequences of a child or young person of a breach of their privacy rights at this developmental stage of their lives include the risk
of trauma, embarrassment or stigmatisation and even the possibility of identity theft.  

Australian law protects privacy, but there are considerable complexities and uncertainties concerning the extent to which it does so. As the Australian Privacy Foundation pointed out in its submission to the cyber-safety committee inquiry:

> The current regulatory models are complex, confusing, often arbitrarily inconsistent between media and jurisdictions, and ad hoc.  

At present, there is no private cause of action that may be brought in Australia specifically for breach of privacy. Instead, privacy may be protected by a combination of private actions – such as defamation, breach of confidence, nuisance, trespass and copyright – and criminal actions – including offences for stalking and harassment. The gaps in the law have led to law reform bodies, including the ALRC, the New South Wales Law Reform Commission (NSWLRC) and the Victorian Law Reform Commission (VLRC), to recommend a statutory cause of action for breach of privacy. Such a cause of action would impose privacy-specific obligations on individuals, such as users of SNS. For example, although it might be possible for a person to bring an action for breach of confidence in relation to a photograph of themselves posted to a SNS, it would probably be easier to bring an action specifically for breach of privacy.

Apart from private causes of action, Australian law protects privacy in a variety of other ways. First, there is a complex patchwork of federal, state and territory laws that protect information privacy. These laws regulate the collection, handling and use of personal information by government and business. There are, however, some important limitations on these laws. In particular, the laws do not impose any obligations on individuals acting in their private capacity. Moreover, they do not apply to small businesses, meaning those businesses with an annual turnover of less than $3 million. There are also important differences between the various federal, state and territory laws. The complexities and inconsistencies associated with this regulatory framework have led to the ALRC recommending major changes to the laws.

Second, there are laws that prevent people from intercepting private electronic communications, such as phone calls and emails. These laws, in general, permit the police to intercept or monitor private communications, but only if they have a warrant.

Third, there are state and territory laws that regulate the use of surveillance devices, such as a CCTV system or cameras in mobile phones, in public places. There are significant differences between these laws in different parts of Australia. For example, in Victoria, devices like surveillance cameras can record any activity outside a building without consent, but consent must be obtained to record a private activity indoors. The VLRC has recommended some changes to the law to increase protection, such as prohibiting surveillance in toilets and change rooms, and preventing a person from recording an activity or conversation to which they are a party without the agreement of the other participants.

Fourth, privacy is also protected by the criminal law. For example, in Victoria it is a crime to engage in stalking or cyber-stalking. Thus, under s 21A of the Crimes Act 1958 (Vic) the offence of cyber-stalking can occur when someone persistently contacts another person by phone or email, or persistently publishes material about that person on the Internet, with the intention of harming them, or causing them to fear for their safety. Criminal laws that create offences for identity theft, and which are explained further below, also play a role in protecting privacy.

---


In its comprehensive review of Australian privacy law, the ALRC recommended that the Office of the Privacy Commissioner, in consultation with ACMA, ‘should ensure that specific guidance on the privacy aspects of using social networking websites is developed and incorporated into publicly available educational material’. The ALRC also recommended that state and territory education departments should ‘incorporate education about privacy, including privacy in the online environment, into school curriculums’. In its submission to the cyber-safety committee inquiry, the Office of the Privacy Commissioner has supported these recommendations.

**Copyright**

SNS are specifically designed to encourage users to create profiles and other pages that represent their interests, hobbies, likes and dislikes. The most common way for users to do this is through the display of images - including photos of themselves, their family and friends – and by posting movie and sound files. Much of the content posted to SNS – and especially material drawn from movies, TV shows, music and other popular culture – is protected by copyright.

In Australia, copyright is created and protected under the *Copyright Act 1968* (Cth) (the Copyright Act). Australia is a member of several international conventions and treaties that oblige Australia to grant copyright protection to materials created overseas. Therefore, even material which is downloaded from a US website will be protected under Australian law.

The Copyright Act provides for the protection of most creative material that is expressed in a material form, including text, music, drawings, photographs, sound recordings, films and broadcasts. Copyright is infringed by doing one of the exclusive rights granted to the copyright owner. For example, with respect to ‘works’, including literary, musical works and artistic works, this includes the exclusive rights:

- to reproduce the work in a material form - meaning to make copies of the material;
- to publish the work - meaning to publish the material for the first time;
- to communicate the work to the public – which includes publishing the material on the internet;
- to make an adaptation of the work – which includes making an arrangement of a musical work.

In order to infringe copyright you need only take a ‘substantial part’ of the work. What amounts to a substantial part is measured mainly by the quality of the part taken, not the quantity, essentially meaning how important the part taken is to the overall work. This means that copyright can be infringed even by using a relatively small piece of someone else’s work. For example, including a musical work as part of a sound track, or a clip from a movie or computer game, in a mash-up video, which is then posted to a SNS, may infringe copyright. Copyright can also be infringed by ‘authorising’ someone else to infringe copyright. This means that a SNS user who posts a link to infringing material and, in particular, allows people to download copyright-protected people, may be liable for authorising the infringements of others.

One of the most controversial issues involving copyright and SNS is the extent to which people should be able to use copyright-protected material in their own creations, such as ‘sampling’ sound recordings or making mash-ups. As copyright may be infringed by taking a substantial

---

part, the use of copyright material in this way is likely to amount to an infringement. While there are a number of defences to infringement, especially defences known as fair dealing, there is no general defence that excuses liability on the basis that the copyright protected material has been used to make a new work. Depending upon the context, a relatively new Australian defence, which allows for fair dealing for the purpose of parody or satire, may provide a defence to some humorous user creations. At present this defence is, however, untested.

As explained above, the ToS of SNS include important terms dealing with the rights and obligations of users in respect to IPRs. For example, the ToS of SNS reviewed for this project all prohibit display of infringing material, or linking to unauthorised material. Users are also required to warrant that the material they upload to a SNS does not infringe the IPRs of third parties. Moreover, reflecting the fact that most SNS are hosted in the US, each site has a notice and take-down policy that complies with the US safe harbour regime. This means that SNS providers reserve the right to remove infringing material. For example, YouTube frequently removes videos uploaded by users on the basis that it has received a notice indicating that the material is infringing.

In addition to using other people’s material, young SNS users create and post their own material, including artwork, short stories, videos and music. Creators of UGC should be aware of the terms and conditions that relate to the content that is posted to a SNS. As explained above, many SNS require users to grant a licence that allows the use of UGC without payment.

**Defamation**

Defamation is the area of law that protects a person’s reputation, which is the way other people see that person, against untrue statements. As defamation protects reputation, it is not whether a person is insulted that is important, but whether some damage is done to the way other people think about the person. Explaining the difference between insulting a person’s character and damaging their reputation, Lord Denning famously said:

> A man’s ‘character’, it is sometimes said, is *what he in fact is*, whereas his ‘reputation’ is *what other people think he is*. (*Plato Films Ltd v Speidel* [1961] AC 1090, 1138.)

In Australia, defamation is unlawful under State and Territory laws which, since 2006, are largely, but not completely, uniform. Civil actions for defamation can be brought against a person who makes a defamatory statement, or someone who publishes a statement. Although prosecutions are rare, defamation is also a criminal offence.

Defamation occurs when someone publishes something that is defamatory about another person. There is a considerable amount of complex law on when something is defamatory, with it sometimes being said that it is anything that exposes a person to “hatred, ridicule or contempt” (*Parmiter v Coupland* (1840) 151 ER 340, 342 per Baron Parke.); or that it is “anything which is likely to cause ordinary decent folk in the community, taken in general, to think less of” the person (*Gardiner v John Fairfax* (1942) 52 SR(NSW) 171, 172 per Jordan CJ.).

As the meaning of a statement can depend upon the context and the circumstances in which it is said, it is impossible to generalise about what might be defamatory. The following are examples of some things that have been held to be defamatory:

- A magazine photograph of the rugby league player, Andrew Ettingshausen (or ‘ET’), in a shower that included his partially obscured penis;
- Suggestions made in a newspaper that a person had smelly feet or was constipated;
- Allegations that the flamboyant Sydney businessman, Rene Rivken, had engaged in sexual intercourse with his male chauffeur;
Photographs of the actors who played Harold and Madge Bishop in *Neighbours*, which were published by an English magazine, and which consisted of the faces of the actors superimposed on the bodies of two people engaged in a bondage session;

An article suggesting that the then captain of the West Indies cricket team, Clive Lloyd, had engaged in match fixing; and

A current affairs television program alleging that a doctor was an ‘abortionist’.

Defamation is committed whenever defamatory matter is communicated to someone other than the person being defamed, provided that the person being defamed is sufficiently identified. Australia’s defamation laws define ‘matter’ broadly to include: articles, reports and advertisements in newspapers and magazines; anything communicated by means of television, radio or the Internet; letters, notes or any other writing; pictures or gestures; or anything at all that can be communicated to a person. Defamation can therefore be committed whenever someone reads a defamatory comment, or views a defamatory photograph or picture, on a social networking site, such as Facebook.

Our research uncovered some evidence of the risks faced by young people when they post unguarded comments to SNS. For example, in an interview conducted with teachers, one of the teachers said:

And some of the language and stuff that they’re willing to share on Facebook in a public forum is not the kind of language and stuff that they would be willing to share in a public room. To go verbatim one might say to another “You f****** slut, I’m going to kill you when I catch up with you next” and the reply to that will be similarly aggressive and profane and yet they wouldn’t do that in front of other people in a real time environment.

Defamation does not prohibit all actions or statements that may damage someone’s reputation, as the protection of reputation must be balanced with protecting freedom of expression. Consequently, there are a number of important defences to actions for defamation, with much of the complexity in defamation law relating to the availability of defences. For example, something is not defamatory if it can be shown that it is substantially true. Moreover, a defendant can argue that an apparently defamatory statement is really fair comment, or an honest opinion.

Although a young SNS user might not think it is very likely that someone sue them for posting potentially defamatory material to a SNS, it needs to be borne in mind that people are very sensitive to defamatory material. For example, quite a lot of disputes have arisen from statements made in community magazines or newsletters produced by small clubs. Young people therefore need to be careful whenever they write something about someone else, or post a photograph of someone else, to a SNS.

A recent South Australian case, which involved a conviction for criminal defamation, illustrates the potential hazards of posting ill-considered, or personally offensive, material to SNS. Christopher Cross, a 19 year old diesel mechanic from Yorketown in South Australia, set up a Facebook group called “Piss Off Mark Stuart”. The Facebook page targeted one of Yorketown’s two police officers, Senior Constable Mark Stuart, who had been active in charging Yorketown locals for driving offences, such as drink driving or driving defective cars. The page included photographs of the police officer, photographs of his children, the location of his house, and 43 posts from members of the Facebook group. Many of the posts about Constable Stuart were offensive or highly defamatory. After an investigation by the Commercial and Electronic Crime Branch of the South Australian police, Cross was charged with criminal defamation.
Given the overwhelming nature of the evidence, Cross pleaded guilty and was convicted, being placed on a two year $500 good behaviour bond. After his conviction, Cross said he “didn’t realise you could get in trouble for things on the internet”.

**Criminal laws: identity theft, harassment & offensive publications**

There are a considerable number of criminal laws that have potential application to use of SNS. In general, these laws fall within the category of criminal law known as cybercrime laws. This project has identified three main categories of cybercrime laws that are especially relevant to SNS use, namely, laws outlawing identity theft, serious harassment or publishing offensive material.

**Identity theft**

Identity theft involves assuming someone else’s identity, usually for the purpose of committing a criminal activity. As the Australian Federal Police submission to the cyber-safety committee inquiry explained:

Data compromised in the online environment may include personal financial information, other personal information such as emails, identity data and photographs. Young person’s details may be used to identify their parents or adult contacts and be subsequently used to attempt to give legitimacy to communications designed to compromise the adults computers or obtain personal and financial details.

Each of the Australian states and territories have introduced relatively new laws that make it an offence to assume or steal another person’s identity. For example, in Victoria, it is a criminal offence to make, use or supply a false ID with the intention of committing on offence; to possess a false ID with the intention of committing an offence; or to possess equipment for making a false ID with the intention of committing an offence. Consequently, it is a crime to take another person’s credit card details with the purpose of buying things without the permission of the credit card owner. There are also other, more traditional, offences that can be committed by the use of a false ID, including theft, criminal fraud or forgery.

**Harassment and menacing**

Commonwealth criminal law includes a number of offences which involve the criminal misuse of telecommunications, including the Internet. The most important crimes are:

- Using a telecommunications network with the intention of committing a serious offence, such as criminal fraud or stalking;
- Using a telecommunications service to make a threat to kill or cause serious harm; and
- Using a telecommunications service to menace, harass or cause offence to a reasonable person.

Each of these offences may be committed by use of technologies such as mobile phones or via SNS. In addition to offences for using the Internet to threaten or harass someone, it is an offence to use telecommunications services, including the Internet, for promoting or inciting suicide. As a result, it is important to understand that rash statements posted to an SNS, which might involve threatening someone or encouraging them to commit suicide, can have potentially serious consequences.

---

The potential liability of young people for the offence of criminal harassment by posting material to a SNS may be illustrated by a recent ACT case, Agostino v Cleaves [2010] ACTSC 19, 3 March 2010. In that case, a 19 year old male defendant became a Facebook friend of another young male through a mutual acquaintance. The defendant had been in a relationship with a young woman that had ended some time before. The other young man started a relationship with the same young woman, and shortly after began receiving threatening messages on his Facebook personal profile site from the defendant. One message read, “You’re a dead dog, ... don’t worry ill (sic) be taking you for a drive really soon don’t forget I know where you live”. The other young man, who was concerned for his safety, ended the relationship with the young woman. Nevertheless, the defendant continued to send threatening messages to him and his friends and relatives. The defendant also posted digital photographs to his own Facebook site, one showing himself holding a replica silver pistol, and one showing the silver gun on a table with five bullets. The other young man contacted the police, who laid charges for using a telecommunications service to menace a reasonable person under s 474.17(1) of the Criminal Code Act 2005 (Cth). The defendant was convicted, and as he was over the age of 18 years, and had a criminal record, he was sentenced to six months imprisonment. An appeal against the sentence was dismissed.

In addition to Commonwealth criminal offences, NSW has introduced a specific offence that applies to harassment or bullying at school. Thus, s 60E of the Crimes Act 1900 (NSW) provides that a person commits an offence if the person assaults, stalks, harasses or intimidates any school student, or member of staff of a school, while the student or member of staff is attending a school, even if no actual bodily harm is occasioned. As the offence applies only to conduct in school premises, however, it may have only limited application to harassment via SNS, or cyber-bullying.

**Offensive material**

Commonwealth criminal law includes a number of offences that cover the use, access, distribution, production and supply of child pornography online. Child pornography is essentially material that is of a sexual and offensive nature that involves people under the age of 18 years. While accessing child pornography online is a federal crime, production and possession of child pornography are crimes under the laws of the states and territories. The Commonwealth crimes extend to child abuse material, which is material that depicts cruelty or physical abuse to a person under the age of 18 years in a way that would be offensive to a reasonable person.

There are harsh penalties for child pornography offences. It is important to understand that posting material that might be classified as child pornography or child abuse, such photos involving sexualised nudity or cruelty, can have very serious consequences. Although child pornography offences were created to protect young people from predatory adults, young people may well commit such offences by engaging in practices such as ‘sexting’. For example, a 14 year old boy from Bunbury in Western Australia was convicted of child pornography charges for distributing footage of a 14 year old girl having sex with two other boys to mobile phones.

In addition to child pornography offences, federal criminal law creates offences for people who are over the age of 18 years to use the Internet for luring or grooming people under the age of 16 years for sexual purposes. These crimes are aimed at preventing adults from taking advantage of young people online.
5.3. **Capacity and liability of minors**

This section of the chapter explains the legal capacity of minors under Australian law, and especially their capacity to enter into binding contracts. It also explains the potential liability of minors for criminal offences.

**Legal capacity**

As explained above, probably the most important legal obligations relating to the use of SNS are those imposed by the ToS of the SNS. It is therefore important to determine the extent to which the ToS are binding on minors.

At common law, a contract with a minor (other than a contract for necessities, *Nash v Inman* [1908] 2 KB 1) is voidable. In Victoria, capacity of minors is dealt with generally under s 7 of the *Goods Act 1958* (Vic), which provides:

*Capacity to buy and sell*  
Capacity to buy and sell is regulated by the general law concerning capacity to contract and to transfer and acquire property:

Provided that where necessaries are sold and delivered to a minor or to a person who by reason of mental incapacity or drunkenness is incompetent to contract he must pay a reasonable price therefore.

Necessaries in this section mean goods suitable to the condition in life of such minor or other person and to his actual requirements at the time of the sale and delivery.

This section, however, applies only to ‘goods’ and therefore does not apply to social networking services, which in any event are unlikely to be considered necessaries. Thus, contracts for services imposed by the SNS providers are likely to be voidable by the students that we interviewed, all being under the age of 18. Nevertheless, we have dealt with the ToS of SNS in some detail in this project as we believe that it is important for young people to become accustomed to familiarising themselves with the online legal obligations they may enter into. Moreover, awareness of the terms incorporated in the ToS of SNS can assist in creating a more general awareness among young people that everyday online activities are not unregulated, but are governed by sometimes complex legal regimes.

**Criminal liability**

In all Australian jurisdictions, children who are 10 years of age or over may be liable for committing criminal offences. Between the ages of 10 and 14 years, however, there is a rebuttable presumption, known as *doli incapax*. This presumption deems a child between the ages of 10 to 14 years as being incapable of committing a criminal act, but can be rebutted by the prosecution showing that a child defendant was, at the relevant time, able to distinguish between right and wrong. From 14 years to either 17 or 18 years (depending on the jurisdiction), young people are considered fully responsible for criminal acts, but will be subject to different criminal penalties to adults.

5.4. **A Modern Parable: Posting Photographs of Naked Footballers**

The potential legal liability of young people for content posted to a SNS was dramatically highlighted in December 2010 by a case in which a 17-year-old Melbourne ex-schoolgirl posted two explicit photographs featuring three prominent Australian football players, two of them
naked, to her Facebook page. The photographs, which had the phrase ‘Merry Christmas courtesy of the St Kilda schoolgirl’ written across them, were evidently part of the teenager’s public ‘campaign’ against the St Kilda football club. Earlier in 2010, the Australian Football League (AFL) and police had interviewed the teenager following unsubstantiated allegations that she had become pregnant to another St Kilda footballer. Although it was initially claimed that the teenager had copied the photographs from the laptop of another St Kilda football player, Sam Gilbert, it was later reported that Gilbert had emailed the photographs to the teenager.

Following the publication of the photographs, on an application to the Federal Court, Marshall J awarded an interim order for the photographs to be removed. While Facebook expeditiously removed the photographs, the teenager immediately posted a link to the photographs on Twitter. The link was removed, but by then the photographs had ‘gone viral’, being copied to multiple Internet sites.

The court orders were emailed to the girl and posted on her Twitter account. Lawyers for the St Kilda football club proceeded to announce that they would take vigorous action seeking to recover damages from the teenager, apparently mainly to deter her from profiting from the incident. St Kilda’s lawyers also posted a message to the girl on the video-sharing web-site, Upstream, advising her to appear at the Federal Court hearing. The girl had been using Upstream to comment on the scandal, as well as to threaten posting further photographs. Subsequently, in an action brought by Gilbert, the Federal Court ordered that the photographs be surrendered to the court on a USB stick, with all other copies destroyed, and required the parties to engage in mediation before 28 January 2011. Subsequently, on 21 January 2011, the St Kilda football club announced an out of court settlement between the teenager and the footballer. Under the terms of the settlement, the teenager agreed to delete all copies of the images and to comply with the court orders, while the football club agreed to provide her with support, including accommodation, for a few months.

The facts in the case present an especially good illustration of the potentially serious legal implications of teenagers posting material, without necessarily appreciating the legal consequences of doing so. In this case, of course, the hazards were exacerbated by the existence of plaintiffs with both the incentive and means to take legal action. Nevertheless, the facts present a useful case study of the range of legal actions that might be available against someone who posts unauthorised photographs to a SNS. The potential actions include actions available to Gilbert, who allegedly took the photographs, actions available to the subjects of the photographs, and potential criminal actions.

First, assuming Gilbert took the photographs, then he would own copyright in the photographs, and copying them and posting them to Facebook without permission would amount to copyright infringement. As Gilbert allegedly took the photographs, he may also have standing to sue the teenager for breach of confidence, if the photographs were, as initially claimed, surreptitiously taken from his laptop. In addition to these actions, the lawyers for Gilbert based their claim on trespass to goods and an action known as intentional infliction of emotional harm. The latter action, which is sometimes pleaded in cases involving breaches of privacy, arises when there is intentional or reckless conduct that causes severe emotional distress. Assuming that Gilbert emailed the photographs to the teenager, he would obviously be less likely to succeed. Nevertheless, depending upon the circumstances in which the

---

photographs were communicated, it would still be possible for the teenager’s actions to amount to breach of copyright and, potentially, a breach of confidence.

Secondly, the footballers featured in the photographs would be entitled to bring actions for breach of confidence and defamation. While the actions of Gilbert, in disclosing the photographs, would clearly amount to a breach of confidence, the teenager could also be liable as a third party in possession of confidential information, particularly if she suspected that the photographs were sent to her in breach of a duty of confidence that Gilbert owed to the featured footballers. Moreover, although there is a defence that allows publication of material in breach of confidence if it is in the public interest, Australian courts have narrowly confined this defence, and it will not apply to material which the public are merely interested in, as opposed to where there truly is a public interest.

In addition to an action for breach of confidence, an action for defamation could be available to the footballers on the same basis as cases such as *Ettingshausen v Australian Consolidated Press Ltd*, which is mentioned at 5.2 above. In that case, the rugby league footballer, Andrew Ettingshausen, successfully brought an action against the magazine, *HQ*, for publishing a photograph of him in a shower which included his partially obscured penis. In any action brought by the subjects of the photographs, unlike Gilbert, they could also plead intentional infliction of emotional harm. Finally, even though, as pointed out at 5.2 above, although Australian law has yet to recognise a self-standing action for breach of privacy, creative pleading could present a claim for the courts to recognise a new action for breach of privacy.

Thirdly, if we leave aside the possibility of criminal actions for defamation or criminal harassment, which have been discussed above, two criminal offences could potentially have applied to the teenager’s conduct. First, if, as initially claimed by Gilbert, the teenager had made unauthorised copies of the photographs from his laptop, an offence could have been committed under s 247G of the *Crimes Act 1958* (Vic), which establishes an offence of unauthorised access to data held on a computer. For this offence to arise, however, the data held on the computer must be protected by an access control system, such as a password. Secondly, if, as apparently initially suggested by the teenager, she was responsible for taking the photographs, an offence may have been committed under Victoria’s so-called ‘upskirting’ laws. In particular, there may have been an offence under s 41C of the *Summary Offences Act 1966* (Vic), which establishes an offence where a person visually captures an image of another person’s genital or anal region and intentionally distributes that image.

While the posting of the photographs to Facebook initiated a series of events with unfortunate consequences for all parties, the publicity given to the events has highlighted the need for greater understand of young people of the potential legal consequences of their actions on SNS. In short, although the use of SNS may have empowering effects in some contexts, this form of social interaction – which, characteristically, blurs distinctions between public and private – is governed by complex laws which do not readily apply to less ‘public’ forms of social interaction, such as face-to-face communications. And, especially where those who suffer harm have both the means and incentive to commence legal actions, potentially serious legal consequences may flow from ill thought-through online conduct. The point of education aimed at promoting understanding of the legal consequences of using SNS is not to spread unfounded fears of using new media, but to empower young users so that they are informed of the laws that apply to their conduct.

---

40 *(1991) 23 NSWLR 443.*
5.5. Conclusion

As this chapter has explained, the everyday use of SNS is subject to a complex range of laws, including laws relating to privacy, copyright, defamation and some areas of the criminal law. These laws either do not apply, or do not apply in the same way, to offline social interactions. Nevertheless, the everyday use of SNS is as spontaneous as off-line interactions. Moreover, SNS interactions leave a more or less permanent record that is not left by off-line social interactions. Consequently, the almost ubiquitous use of SNS by young people gives rise to legal risks that have not been encountered by previous generations. When combined with some elements of a culture that encourages unconstrained expression online, there is the possibility of young users suffering potentially serious consequences. The experiences of the young woman at the centre of the St Kilda photograph scandal provide an illustration of what can happen when things go awry.

Although, as explained in this chapter, the areas of the law that may be implicated in the everyday use of SNS are complex, a general understanding of the kinds of legal risks associated with everyday SNS use would assist all users, not just young SNS users, in managing those risks. As explained in other parts of this report, the objective in dealing with the legal risks of SNS use is not to inhibit the use of SNS, nor to promote a safety-first culture that is dominated by the fear of risks. It is, rather, to assist users in being able to appropriately understand and manage legal risks, so as not to compromise the benefits of SNS use.
6. Regulatory & Policy Responses

This chapter of the report identifies and explains the regulatory responses to the risks faced by young people using SNS, so as to inform the recommendations to be made in Chapter 7 regarding regulatory steps that could potentially be adopted in Australia. Before doing so, however, the chapter identifies the objectives of regulating SNS, especially as these relate to the protection of young users. The chapter then reviews the main regulatory initiatives that have been taken in the US and Europe, which have been the main jurisdictions in which initiatives specifically directed at SNS have been introduced. Following this, the chapter explains the main initiatives and policy responses to SNS that have been introduced in Australia to date. The chapter concludes with a summary and some general observations regarding the regulation of SNS to deal with legal risks facing young people.

6.1. Objectives of Regulating SNS

Discussions of the use of SNS by children and young people are understandably focused on fears of the risks that unregulated online social interactions may pose to the vulnerable, such as cyber-bullying and inappropriate contacts from adult predators. Nevertheless, it is important to appreciate the significant potential benefits for young people that may arise from the use of new social media. For example, a report produced as part of the landmark MacArthur Foundation digital media and learning initiative identified the following potential benefits from the use of new social media by young people:41

- **Social and recreational new media use as a site of learning** – it is important to appreciate that young people who are interacting socially online are accumulating social and technological skills that are needed to participate in contemporary society.

- **Diversity in forms of media literacy** – online interactions range from purely friendship-driven to interest-driven, but each may have benefits in terms of socialising or education that are necessary for participation in future social or work environments.

- **Peer-based learning** – use of new media facilitates learning from peers, which has some advantages over learning from adults, including teachers.

- **Changing role of education** – the participation of young people in social media presents important new learning opportunities, if educational practices can harness the power of the new social tools.

As a submission to an inquiry conducted by the US Federal Communications Commission (FCC), produced by the Youth and Media Policy Working Group Initiative at Harvard University, succinctly put it:

As we seek to protect youth from the unforeseen risks of online engagement, it is essential that we do not in turn foreclose the benefits made possible by self-directed,

---

informal learning and socializing through new technologies or experimentation with teaching using new technologies in the classroom.\textsuperscript{42}

In the notice soliciting comments for its inquiry, the FCC included a useful summary of the key benefits and potential risks facing young people in the use of the new social media.\textsuperscript{43} The most important benefits identified by the FCC are:\textsuperscript{44}

- Access to educational content;
- Acquiring technological literacy needed to compete in a global economy;
- Developing new skills in the use of technology and the creation of content;
- Facilitating new forms of communication with family and peers; and
- Removing barriers for children with disabilities.

On the other hand, there is no doubt that use of SNS expose children and young people to new risks, or to new forms of old risks. In its notice, for example, the FCC identified the following main risks associated with the use of new social media by children and young people:

- Exposure to inappropriate content (including offensive language, sexual content, violence, or hate speech).
- Potential impact on behaviour;
- Harassment and bullying;
- Sexual predation;
- Fraud and scams;
- Failure to distinguish between who can and who cannot be trusted when sharing information;
- Compromised privacy; and
- Exposure to exploitative advertising, or use of user information, by SNS providers.

To these, we would add a lack of adequate awareness of the potential legal risks that may arise from participating in SNS.

Given the benefits of youth engagement in SNS, the role of regulating SNS is essentially to protect children by minimising the risks facing children and young people who use SNS, while not compromising the benefits. In pursuing this objective, any potential regulation faces a number of important challenges. First, the technology is rapidly changing, and even more so, so are the social conventions relating to the use of SNS. This means that SNS use, and the associated risks, are really a moving target. Secondly, there is a diversity of SNS, with different services providing quite different products. It is therefore impossible to impose ‘one size fits

\textsuperscript{44} \textit{Ibid.} p. 6.
all’ regulatory solutions. Thirdly, most important SNS providers are headquartered outside of Australia, meaning that there are limits on the extent to which Australian authorities can influence their behaviour. Fourthly, the use of SNS by many young people has become so embedded in their lives, that there is likely to be some resistance to some attempts to introduce new rules.

These factors suggest that a nuanced and finely-tuned approach must be adopted to regulation aimed at minimising the risks faced by children and young people using SNS. This would seem to necessarily entail a multi-pronged approach, with an emphasis on educating young people, but also some potential role for governments to influence the behaviour of SNS service providers. The next sections of the chapter explain some of the major policy initiatives that have already been introduced in this area.

6.2. US Initiatives

This section of the chapter explains the main initiatives that have been taken to regulate the risks posed to children by SNS in the US. To date, US regulatory initiatives have consisted mainly of official reports, information gathering exercises and educational initiatives, while there has been very little in the way of direct regulation.

The extent to which material on SNS can be regulated in the US is constrained by the protection given to free speech under the First Amendment to the US Constitution. Although there is some uncertainty relating to the legal standard to apply to the regulation of school-related speech, it appears that ‘off-campus’ speech is protected to a much greater extent than ‘on-campus’ speech, which may be regulated to prevent disruption to the school environment. As Heidlage has correctly pointed out, drawing a line based largely upon the physical location of the speech creates real difficulties for the regulation of school-related speech on the Internet, including postings by students about their teachers.

Although the First Amendment sets important limits on the regulation of SNS in the US, state governments in the US were among the first to respond to concerns about the risks posed by SNS to children. The first important initiative in this area was the Joint Statement on Key Principles of Social Networking Safety, which was an agreement between MySpace and the Attorneys General representing 49 states and the District of Columbia in January 2008. The Statement, which is non-binding, adopted the following principles:

- Providing children with a safer social networking experience is a primary objective for operators of social networking sites.
- Technology and other tools that empower parents, educators and children are a necessary element of a safer online experience for children.
- Online safety tools, including online identity authentication technologies, are important and must be robust and effective in creating a safer online experience, and must meet the particular needs of individual Web sites.

---

45 Ibid.
46 Tinker v Des Moines Independent Community School District, 393 US 503 (1969); Bethel School District No. 403 v Fraser, 478 US 675 (1986); Morse v Frederick, 127 S Ct 2618 (2007).
• Development of effective Web design and functionality improvements to protect children from inappropriate adult contacts and content must be an ongoing effort.

• Educating parents, educators and children about safe and responsible social networking site use is also a necessary part of a safe Internet experience for children.

• Social networking site operators and law enforcement officials must work together to deter and prosecute criminals misusing the Internet.

Pursuant to the Joint Statement, the parties agreed to establish an Internet Safety Technical Task Force (ISTTF), to consider the extent to which technologies can enhance the safety of minors in online spaces, such as SNS. The ISTTF, which was chaired by John Palfrey, Dena Sacco and danah boyd from the Berkman Center for Internet & Society, released its Final Report in December 2008 (ISTTF). The ISTTF report made two major findings: first, that ‘[s]exual predation on minors by adults, both online and offline, remains a concern’; and, secondly, ‘[b]ullying and harassment, most often by peers, are the most frequent threats that minors face, both online and offline’.

The report included a comprehensive set of recommendations, including recommendations for: the Internet community; the expenditure of increased resources to enhance child safety; and parents and caregivers.

The recommendations for the Internet community included that members of the Internet community should work with child safety experts, technologists, public policy advocates, social services and law enforcement to:

• develop and incorporate a range of technologies as part of their strategy to protect minors from harm online;

• set standards for using technologies and sharing data;

• identify and promote best practices on implementing technologies as they emerge and as online safety issues evolve; and

• put structures into place to measure effectiveness.

The recommendations for increased resources identified the need for allocating greater resources:

• to schools, libraries, and other community organizations to assist them in adopting risk management policies and in providing education about online safety issues;

• to law enforcement for training and developing technology tools, and to enhance community policing efforts around youth online safety; and

• to social services and mental health professionals who focus on minors and their families, so that they can extend their expertise to online spaces and work with law enforcement and the Internet community to develop a unified approach for identifying at-risk youth and intervening before risky behavior results in danger.

Finally, the major recommendations for parents and caregivers included:


50 Ibid. 4.
• Parents and caregivers should educate themselves about the Internet and the ways in which their children use it, as well as about technology in general.

• Parents and caregivers should explore and evaluate the effectiveness of available technological tools for their particular children and family context, and adopt those tools appropriately.

• Parents and caregivers should be engaged and involved in the Internet use of their children, discussing it from an early age, setting appropriate limits and instilling good behaviour from the start. Being attentive to early signs of harassment, both in terms of children as bullies and victims, is critical, especially because bullying tends to escalate over time.

• Parents and caregivers should be conscious of the common risks that minors face and avoid focusing on rare or hypothetical dangers. Their strategies should centre on helping their children understand and navigate the technologies and creating a safe context in which their children will turn to them when there are problems. Trust and open lines of communication are often the best tools for combating risks.

• Parents and caregivers should be attentive to at-risk minors in their community and in their children’s peer group.

While the Joint Statement and the ISTTF were specifically directed at SNS, there have been a range of relatively fragmented initiatives directed at promoting the safety of children in the online environment more broadly. The most important federal US legislative initiatives in this area have been:

• The Children’s Online Privacy Protection Act,\(^5\) which requires the Federal Trade Commission (FTC) to adopt regulations regarding the responsibilities of web-sites operated for commercial purposes that collect information from children under the age of 13 years.

• The Adam Walsh Child Protection and Safety Act of 2006,\(^5\) which mainly deals with registration of sex offenders, but which authorises the federal Attorney-General to carry out a public awareness campaign to demonstrate to children, parents and community leaders how to protect children on the Internet.

• The Broadband Data Improvement Act,\(^5\) which mainly deals with the collection of data on broadband availability in the US, but which directed the National Telecommunications and Information Administration (NTIA) to establish the Online Safety and Technology Working Group (OSTWG) to examine industry efforts to promote online safety through educational efforts; and requires the FTC to carry out a nationwide program to increase public awareness and provide education about strategies to promote safe use of the Internet by children.

Pursuant to its mandate under §214 of the Broadband Data Improvement Act, the NTIA established the OSTWG to review and evaluate:\(^5\)

• The status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies or initiatives designed to promote a safe online environment for children;

• The status of industry efforts to promote online safety among providers of electronic communications services and remote computing services by reporting apparent child pornography, including any obstacles to such reporting;

• The practices of electronic communications service providers and remote computing service providers related to record retention in connection with crimes against children; and

• The development of technologies to help parents shield their children from inappropriate material on the Internet.

In June 2010, the OSTWG released a major report which made recommendations on youth online safety. The report made general recommendations, as well as more specific recommendations that were derived from four OSTWG sub-committees. The OSTWG’s general recommendations were:

• Studies of child online safety need to be properly resourced;

• The recommendations made in the report need to be followed up;

• A coordinating body needs to be formed to build consensus and coordinate the efforts of government agencies, industry and NGOs;

• A full review of all federal government child online safety projects and programs must be undertaken; and

• A multi-stakeholder approach is needed to deal with the complex issues raised by child online safety, as no single stakeholder has the required expertise.

The specific recommendations of the OSTWG sub-committee on Internet safety education were to:

• Keep up with the youth-risk and social-media research, and create a web-based clearinghouse that makes this research accessible to all involved with online safety education at local, state, and federal levels.

• Coordinate Federal Government educational efforts.

• Provide targeted online-safety messaging and treatment.

• Avoid scare tactics and promote the social-norms approach to risk prevention.

• Promote digital citizenship in education as a national priority.

• Promote instruction in digital media literacy and computer security in education nationwide.

• Create a Digital Literacy Corps for schools and communities nationwide.

• Make evaluation a component of all federal and federally funded online safety education programs (evaluation involving risk-prevention expertise).

• Establish industry best practices.
• Encourage full, safe use of digital media in schools’ regular instruction and professional development in their use as a high priority for educators nationwide.

• Respect young people’s expertise and get them involved in risk-prevention education.

The other sub-committees established by the OSTWG were sub-committees on parental controls and child protection technology, child pornography reporting and data retention.

The FTC, which is the federal US agency responsible for consumer protection and privacy, performs an important role in promoting public education on Internet safety. In particular, it hosts OnGuard Online, which is a partnership of 11 federal agencies and 17 groups that provide educational material, videos and games to protect against email scams, identity theft, kids privacy, SNS, spyware and phishing.55

The Federal Communications Commission, which is the US federal agency responsible for regulating electronic communications, has also taken a strong interest in protecting children online. In October 2009, the Federal Communications Commission (FCC) published a Notice of Inquiry (NOI), entitled Empowering Parents and Protecting Children in an Evolving Media Landscape, seeking information about the benefits and risks for children of new electronic media technologies.56 This was a wide-ranging inquiry, with a specific focus on soliciting information about how improvements in new media literacy could assist in dealing with online risks. While submissions to the NOI elicited valuable information, the extent to which the FCC has legislative authority to regulate electronic media other than broadcasting and cable TV is quite uncertain.57

Although the US initiatives reviewed in this report are far from comprehensive, they share some common features. First, the initiatives mostly adopt an approach of appropriately managing risks, rather than inhibiting use. Secondly, in doing so, the initiatives recognise that appropriately managing risks is a complex task, which involves the interaction of multiple stakeholders, including governments, SNS operators, parents and responsible adults, and children themselves. In particular, the US initiatives generally see the role of government as one of encouraging and facilitating industry-based developments, rather than directing industry to take action. Thirdly, given the diversity of SNS, and the constant evolution of the enabling technologies, the initiatives mostly acknowledged that there can be no ‘one size fits all’ regulatory policy. Fourthly and finally, the US initiatives and studies agree that any sophisticated regulatory response must include a combination of modalities, such as education, technologies (such as authentication technologies), self-regulatory codes, and policies implemented through conditions of use imposed on users.

While acknowledging the need for a multi-pronged approach to risk management, the US initiatives all clearly recognise the importance of ensuring that the benefits of SNS are not destroyed by inappropriate regulation. For example, the ISTTF report makes the following points, which are important for potential regulators to bear in mind:

Not all interactions between adults and minors are unhealthy and potential solicitations … Minors gain benefits by being able to engage in healthy and supportive interactions with adults, including known adults and adults who are participating

57 See, for example, In the Matter of Empowering Parents and Protecting Children in an Evolving Media Landscape, Comments of Progress & Freedom Foundation (PFF) & Electronic Frontiers Foundation (EFF), 24 February 2010.
alongside youth in communities of interest ... Excluding teachers and other role models from sites could have unintended consequences for learning and development.\textsuperscript{58}

In sum, then, the US initiatives in this area have focussed mainly on information gathering and promoting online safety education and digital literacy. There has, however, been a degree of fragmentation in the US initiatives, with a lack of coordination between the steps taken by different government agencies. There also appears to be a lack of rigorous analysis of the extent to which industry is attempting to assist with initiatives such as the 2008 Joint Statement.

6.3.  European regulatory initiatives

This section of the chapter explains the main regulatory and policy initiatives that have been implemented in Europe. In understanding this material, it is important to appreciate that the Europe-wide initiatives may be both implemented and supplemented by initiatives at the national level in EU member states.

To date, there have been more proactive policy initiatives directed at the regulation of SNS in Europe than in any other part of the world. This arises, in part, from the overarching legal framework for the regulation of SNS in Europe, which differs considerably from that in the US. In particular, Europe does not have the same constraints on the regulation of SNS content as there are in the US as a result of the influence of the First Amendment. Moreover, there is generally a much greater emphasis on privacy protection in Europe, which can entail strong government intervention.\textsuperscript{59}

The most important regulatory initiative undertaken by the European Union (EU) that specifically relates to the protection of children in the use of SNS is a set of seven principles, known as the \textit{Safer Social Networking Principles for the EU}.\textsuperscript{60} The principles, which are effectively a form of self-regulation, were developed by SNS providers in consultation with the European Commission, and were voluntarily adopted by the major online social networks active in Europe on ‘Safer Internet Day’ in February 2009. The seven principles, which have been agreed to by 20 leading SNS providers, including Bebo, Facebook, Google/YouTube, Myspace and Sulake.Habbo Hotel, are set out in Table 35.

<p>| Table 35  |</p>
<table>
<thead>
<tr>
<th>Safer Social Networking Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Principle 1</strong></td>
</tr>
<tr>
<td><strong>Principle 2</strong></td>
</tr>
<tr>
<td><strong>Principle 3</strong></td>
</tr>
<tr>
<td><strong>Principle 4</strong></td>
</tr>
</tbody>
</table>


As part of the commitment to implementing the self-regulatory principles, the signatories agreed to provide to the European Commission a self-declaration on how they complied with the principles. In January 2010, the European Commission published a report, prepared by Staksrud and Lobe, evaluating the implementation of the Safer Social Networking Principles. The report evaluated the principles by analysing the self-declaration reports submitted by SNSs and testing the corresponding SNS services. In all, twenty-two to twenty-five services were tested for compliance with the different principles. Some of the more important findings of the report on compliance with the seven principles are set out in Table 36.

Table 36
Evaluation of Implementation of Safer Social Networking Principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Evaluation</th>
</tr>
</thead>
</table>
| Principle 1 | - While most services give sufficient information on Terms of Service, three services gave no information and four services had no information on their privacy policy.  
- Safety information for younger children was difficult or impossible to understand on one third of all services that provided such information.  
- Information for parents and teachers was made available on 16 services, but safety tips for teachers was found on only five services.  
- Regarding specific risks, information on online bullying, information privacy and hate speech was most commonly found, followed by information on the risk of posting sexually provocative photographs.  
- Of twenty-five sites evaluated, very few had information on the risks of inappropriate contact from adults, the possibility of seeing or being the subject of child abuse images, or information on self-harm actions. |
| Principle 2 | - E-mail verification from the user or user’s parent was required on twenty services, but seven of those services actually enabled sign up without confirmation.  
- For sites that purport to deny signing up 11 year olds, access was granted on seven services merely by changing the date of birth, while retaining the same profile. If a user attempted to sign up with a new profile, but from the same computer, all sites tested granted access. |
| Principle 3 | - Although fourteen of the SNSs declared that profiles are set to private by default for users under 18 years, only seven actually did so.  
- On eight of the services it was possible to search for users or user profiles that are 12 years or younger on the service itself. |

Principle 4

- Nineteen of the services had a link or information available at all times on where to report content that bothered the user or violated the Terms of Service.
- The reporting mechanism on fifteen of the services was considered easy to understand for children and young people, but eight were considered not to be.
- Fourteen of the twenty-two services tested complied with the recommendation of acknowledging reports from users.
- Of the twenty-two services tested, thirteen did not reply to a message from an underage user asking for help sent through their reporting mechanism, while two replied within a week, with only seven replying within 24 hours.

Principle 5

- A majority of the services reported that they shared reports of illegal content or conduct with law enforcement bodies.
- A majority also explicitly stated that they had effective processes for reviewing and removing illegal content or conduct.
- For ethical reasons Principle 5 was not independently tested.

Principle 6

- Users were usually required to submit their e-mail, real name and gender when signing up to a service.
- The most frequently automatically uploaded personal information was gender and name, followed by age.
- Four services allowed users to submit a personal identification number, and asked for political and religious affiliations.
- Information on how users can delete their profile was found on eighteen of twenty-five services. On five of the services, however, the profile could not be deleted, but only deactivated.
- Eight of the twenty-five services reviewed provided information on how personal information might be used by the service after the user’s profile is deleted.
- Eight of the services provided users with safety tips or information about publishing personal information.

Principle 7

- Most services reported having either human or automated forms of moderating for illegal or prohibited content or conduct.
- Only five of twenty-four services reported taking steps to minimise the risk of employing human moderators that may be unsuited for real-time contact with children and young people.
- For ethical and practical reasons Principle 7 was not independently tested.

The European regulatory approach to SNS places considerable emphasis on privacy and data protection. The first initiative directed specifically at SNS was the Rome Memorandum, which was adopted by the Berlin International Working Group on Data Protection in Telecommunications in March 2008.62 The Working Group, which was established in 1983 by European data protection commissioners to improve the protection of privacy in telecommunications, publishes recommendations including common positions and working

---

papers. The Memorandum, which set out guidance on protecting privacy in SNS, emphasised the risks associated with SNS, including:

- **No oblivion on the Internet** – meaning the persistence of data on the Internet.
- **The misleading notion of “community”** – which may lead to users thoughtlessly revealing their personal information.
- **“Free of charge” may in fact not be “for free”** – meaning that personal information revealed on SNS may, in fact, be the price paid for using the service.
- **Traffic collection by SNS providers** – which refers to the technical ability of service providers to monitor and collect personal information.
- **Misuse of profile data by third parties** – referring to the ease with which personal data included on user profiles may be accessed and copied.
- **Increased risk of identity theft**.
- **Use of a notoriously insecure infrastructure by SNS providers** – including well-publicised security breaches by prominent SNS providers.

Since the *Rome Memorandum*, European Union institutions have given attention to promoting initiatives to protect the privacy of children in using SNS. For example, in February 2009, the Working Party established under Article 29 of the European Data Protection Directive published a comprehensive Opinion on the protection of children’s personal data, with special guidance on the use of data for schools. The Opinion, which was based on the need for taking into account the best interests of the child as required by the UN Convention on the Rights of the Child, included the following statement of objectives:

Children and pupils should be brought up to become autonomous citizens of the Information Society. To this end, it is crucial that they learn from an early age about the importance of privacy and data protection. These concepts will enable them later to make informed decisions about which information they want to disclose, to whom and under which conditions. Data protection should be included systematically in school plans, according to the age of the pupils and the nature of the subjects taught.

Subsequently, in June 2009, the Working Party adopted an Opinion on online social networking. The social networking Opinion built on the earlier Opinion on the protection of children’s data to propose a multi-pronged strategy for protecting children’s data in the SNS context. In particular, the Opinion recommended that the strategy include the following elements:

- **Awareness raising initiatives**, including the introduction of privacy basics in educational curricula;
- **Fair and lawful processing** of the data of minors, including not asking for sensitive data in subscription forms, no direct marketing aimed at minors, and suitable degrees of logical separation between the communities of children and adults;

---


- Implementation of Privacy Enhancing Technologies (PETs), such as privacy-friendly settings by default;
- Self-regulation by providers, to encourage the adoption of codes of practice that should be equipped with effective enforcement measures; and
- If necessary, legislative measures to discourage unfair or deceptive practices in the SNS context.

Meanwhile, in May 2009, the European Commission launched a comprehensive review of the European data protection legal framework, especially to deal with the challenges of rapid technological developments and globalisation. As part of this process, on 4 November 2010 the European Commission released a strategy for reform of data protection laws for public comment, with a view to proposing legislation in 2011. While the review is wide-ranging, the strategy is particularly concerned with the possibility of introducing mechanisms to enhance control over personal data. In this respect, the strategy specifically pointed to problems encountered by users in attempting to have personal data retrieved or deleted from SNS. The strategy therefore flagged the need for clarification of what has become known as the ‘right to be forgotten’, meaning ‘the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes’.

Despite the considerable differences in emphasis in the overall regulatory approaches adopted in the US, on the one hand, and the EU, on the other, there are important common elements. Like the US initiatives, the European regulatory initiatives acknowledge the importance of educators in promoting the responsible use of SNS. For example, the Safer Social Networking Principles state that:

Teachers and other carers … play a crucial role in promoting the safe use of SNSs by children and SNS providers should ensure that such materials also empower teachers to help children use SNSs safely and responsibly.

Moreover, like the US initiatives, the European approach acknowledges the importance of cooperation between multiple stakeholders (including SNS providers, educators and students), and of adopting a user-oriented, nuanced approach to regulation, including elements of education, self-regulation and user empowerment. Notably, as with the US initiatives, the positive role of educators engaging with children in the responsible use of SNS is given a degree of prominence in the suite of available regulatory responses to the risks posed to children by SNS.

6.4. Australian initiatives

In Australia, the use of SNS by young people is generally dealt with by means of a range of policies adopted by Commonwealth, State and Territory education departments directed at promoting cybersafety. These initiatives occur within a framework in which some attention has been given to the protection of children and young people online at the Commonwealth level.

66 Ibid. p 8.
Australia has an extraordinarily complex regime, established under Schedule 7 of the Broadcasting Services Act 1992 (Cth) for regulating Internet content with an Australian link.68 The regime essentially provides for the removal of certain Internet content, known as prohibited content or potential prohibited content, which is either stored in Australia or streamed from Australia, in response to complaints. The content that is prohibited under the regime is content that is either classified, or is likely to be classified, as Refused Classification (RC) or X 18+. In addition, access to R 18+ (Restricted) content must be subject to a restricted access system, as must access to MA 15+ material provided by a commercial web-site. A restricted access system, which is provided for by the Restricted Access Systems Declaration 2007, determined by the Australian Communications and Media Authority (ACMA), is essentially an age verification mechanism designed to ensure that content is not accessible to under-age people.

While the complex Australian regime for regulating information privacy does not expressly deal with the privacy of young people, a comprehensive 2008 report produced by the Australian Law Reform Commission (ALRC) addressed the issue of young people and SNS.69 The report acknowledged that there are legitimate concerns about the use of SNS by young people, but considered that it was neither practical nor desirable to regulate individual non-commercial activities in the on-line environment.70 In addition, while the ALRC noted the value of self-regulatory initiatives, such as those introduced in Europe, it pointed out that they were unlikely to substantially inhibit young people from making ‘bad privacy choices’ online.71 After assessing the available options, the ALRC emphasised the importance of undertaking systemic educational initiatives relating to the privacy implications of SNS. In this respect, the ALRC’s report stated that:

The ALRC considers that the most effective measure that can be taken at present is to educate children, young people, teachers and parents about social networking websites. Education in this area should highlight the privacy dangers associated with the disclosure of personal information on social networking websites and should provide advice on how to use these websites safely and appropriately.72

Following from this, the ALRC report made the following two specific recommendations:

- The Office of the Privacy Commissioner, in consultation with the Australian Communications and Media Authority, should ensure that specific guidance on the privacy aspects of using social networking websites is developed and incorporated into publicly available educational material.
- In order to promote awareness of personal privacy and respect for the privacy of others, state and territory education departments should incorporate education about privacy, including privacy in the online environment, into school curriculums.73

Specifically in relation to cyber-safety and young people, a Joint Select Committee on Cyber-Safety was established by the Commonwealth House of Representatives and Senate in September 2010. The terms of reference of the Committee were to inquire into and report on:

---

70 Ibid. p 459.
71 Ibid. p 2250.
72 Ibid.
73 Ibid. p 2252.
i. the online environment in which Australian children currently engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles) and stakeholders controlling or able to influence that engagement (governments, parents, teachers, traders, internet service providers, content service providers);

ii. the nature, prevalence, implications of and level of risk associated with cyber-safety threats, such as:
   - abuse of children online (cyber-bullying, cyber-stalking and sexual grooming);
   - exposure to illegal and inappropriate content;
   - inappropriate social and health behaviours in an online environment (e.g. technology addiction, online promotion of anorexia, drug usage, underage drinking and smoking);
   - identity theft; and
   - breaches of privacy;

iii. Australian and international responses to current cyber-safety threats (education, filtering, regulation, enforcement) their effectiveness and costs to stakeholders, including business;

iv. opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with cyber-safety issues;

v. examining the need to ensure that the opportunities presented by, and economic benefits of, new technologies are maximised;

vi. ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bullying including by:
   - increasing awareness of cyber-safety good practice;
   - encouraging schools to work with the broader school community, especially parents, to develop consistent, whole school approaches; and
   - analysing best practice approaches to training and professional development programs and resources that are available to enable school staff to effectively respond to cyber-bullying;

vii. analysing information on achieving and continuing world’s best practice safeguards;

viii. the merit of establishing an Online Ombudsman to investigate, advocate and act on cyber-safety issues.

There has been quite a range of cybersafety initiatives that are applicable to schools, which have been introduced by Commonwealth, State and Territory education departments. The most important initiatives implemented in the various jurisdictions are as follows.

**Commonwealth**

At the Commonwealth level, the Department of Education, Employment and Workplace Relations (DEEWR) provides guidance on a national approach to the use of ICT in schools, and to address the issues of bullying, harassment, violence, and child abuse and neglect. The two most important Commonwealth policies are:

- *Better Practice Guide: ICT in Schools* – was developed to assist schools with decisions about the deployment of ICT. The guide is designed to feed into each school’s individual ICT plan.
• **National Safe Schools Framework (NSSF)** – was developed by the Ministerial Council on Education, Employment, Training and Youth Affairs to provide an agreed national approach to the issues of bullying, harassment, violence, and child abuse and neglect. The NSSF is currently under review.

**New South Wales**

The main initiatives implemented by the NSW Department of Education and Training are as follows:

• An Internet filtering system, known as SmartFilter, was introduced to all NSW schools in 2007.

• Memorandums and Legal Issues Bulletins, including advice on the use of ICTs, are distributed to school principals, education directors and regional directors.

• The *Student Welfare Policy*, introduced in 1996, requires all NSW government schools to have an Anti-bullying Plan.

• The *Online Communications Services: Acceptable Usage for School Students* policy, introduced in 2006, defines the policy for acceptable use of Internet and online communication services provided by the Department.

**Victoria**

The main initiatives developed by the Victorian Department of Education and Early Childhood Development are as follows:

• A web-site, known as *Working with the Web*, has been developed as a guide to ethical and safe use of the Internet in Victorian schools. The web-site includes recommendations and resources to help schools: develop school policy and practices surrounding cyber safe and ethical use of the internet; manage and use the internet across the school including the school website; understand online legalities, including those related to digital copyright and online privacy; and plan curriculum involving the internet.

• Forms and templates have been made available for schools to develop their own Acceptable Use Guidelines, which include duty of care requirements.

• A range of resources have been made available to promote cybersafe classrooms.

• The Department has introduced a *Safe Schools are Effective Schools* strategy, which includes anti-bullying guidelines and policies.

**Queensland**

Independent Schools Queensland has developed a number of policies that can be used by individual schools to tailor their own cybersafety policies, including:

• *Child Protection Policy* – which covers reporting of abuse or neglect of children, and how to protect young people from inappropriate behaviour, harassment and self-harm. This is supplemented by the *Child Protection Compliance Policy*.

• *Anti-bullying Policy* – which is designed to ensure that students and staff feel safe from bullying, including cyber-bullying.

• *Computer Use Policy* – which outlines protocols and procedures for the use of schools’ electronic communication facilities and computers, including acceptable use policies.
The Queensland Catholic Education Commission also has a range of policies that incorporate policies and position relating to cybersafety issues.

**South Australia**

The Department of Education and Children’s Services launched a cybersafety initiative in July 2009, which is centred on a set of guidelines for schools and preschools, called *Cyber safety: Keeping Children Safe in a Connected World*. The guidelines have three main elements:

- Preventing risks to children and young people online through classroom learning, as detailed in the *Keeping Safe: Child Protection Curriculum*.
- Security measures to ensure that learning networks are used appropriately, which include acceptable use policies.
- Procedures for suspension and exclusion of students who behave in a threatening manner, even if the event occurred outside of school or outside school hours.

There are different templates for acceptable use policies for pre-school, primary school and secondary school years. The Department also requires all schools to have anti-bullying policies in place. The South Australian Commission for Catholic Schools also has a number of overarching policy documents that are relevant to cyber-safety, but which must be implemented by each school in the Catholic sector.

**Western Australia**

The Department of Education and Training has produced policies for individual schools to develop appropriate use, mobile phone and cyber-bullying policies, as well as guidelines for implementing the policies. The Department has introduced the following curriculum initiatives: ICT in learning; Student online safety; and Cyber-bullying curriculum resources. The Department also has a project dedicated to promoting Internet safety of all public school students. Separate cybersafety programs are administered by the Association of Independent Schools (WA) and the Catholic Education Office (WA).

**Tasmania**

The Department of Education provides the following resources:

- *Web Safety Kit for Schools* – which includes material based on the Victorian *Working with the Web* web-site.
- *Web Safety Policy* – which is designed to ensure that Tasmanian students participate safely in technology-based learning.
- *Web Filtering Policy*.
- A guide, recommendations and resources to support schools developing their own cyber-safety policies and curriculum.
- Resources for addressing cyber-bullying.

**Australian Capital Territory**

The ACT Department of Education and Training has developed policies relating to:

- Acceptable Use of ICT.
- Appropriate Use of Mobile Phones.
• Providing Safe Schools.
• Countering bullying, harassment and violence in ACT public schools.

The Department uses Internet filtering software, and has published a guide for ACT parents, entitled *Keeping Children Safe in Cyberspace*.

**Codes of Conduct**

While the various cybersafety initiatives are aimed at educating and protecting students, teachers’ use of SNS is governed by professional codes of conduct, which differ considerably between the States and Territories. To date, the most direct and restrictive approach to teachers’ use of SNS is found in the Queensland Department of Education and Training *Code of Conduct*. Principle 2.2.2 (b) of the Code, which deals with interactions with students, specifically provides that:

> You must not use internet social networks such as *Face Book, My Space or YouTube* to contact or access present students enrolled in any school or institute.

The Codes of Conduct in other States and Territories are less prescriptive. For example, Principle 1.5(d) of the *Victorian Teaching Profession Code of Conduct*, states that a professional relationship with a student will be violated if a teacher:

> holds conversations of a personal nature or has contact with a student via written or electronic means including email, letters, telephone, text messages or chat lines, without a valid context.

Houey has suggested that, in practice, this means that:74

1. Teachers should only have online communication with a student if it is bona fide about school work.
2. Teachers are at risk of rumour, innuendo, blurring of boundaries and disciplinary breaches if they do more.
3. It is not the role of teachers to be accessible to students 24/7, even in the digital age!
4. The teacher-student relationship is always there – it cannot and must not change.

Melanie Saba, CEO of the Victorian Institute of Teaching, who was one of the experts interviewed for this project, noted that two main issues arose with respect to teachers using SNS for personal purposes:

There are two issues here:

i. a teacher who is a member of a social networking site needs to be mindful that any content posted to the site including comments, photographs and videos, might be accessible to other members of the site or to the public. Any inappropriate material or comments could be the subject of an inquiry by the Institute (eg where a parent, another teacher or a student complains to the Institute about the material) and may result in disciplinary action taken against the teacher;

ii. the second issue is whether a teacher should communicate with a student on a social networking site. As noted above, the Code explains that such activity will violate the teacher’s professional relationship with the student if there is no valid context.

A blanket prohibition on use is likely to be far less effective than equipping users with a sound ability to deal with and report any troubling behaviour. Similarly, some clearer guidance needs to be given to teachers regarding uses that are permissible. The results of the project discussed above indicate that it may be useful for both teachers and students to identify some aspects of SNS ‘space’ that they can share to enable teachers to meaningfully discuss the benefits and risks of what has come to be a ubiquitous communications environment. Thus the underpinning principles of regulation, including any relevant codes of conduct should be user empowerment and education.

6.5. **Summary**

This chapter has canvassed a range of regulatory responses to the risks encountered by young people in their use of SNS. While these responses may reflect varying cultural contexts, they place a common emphasis on the importance of educating young people, their parents and teachers about the safe use of SNS and the broader internet environment. Recognising that the need to equip young users with the skills necessary to take advantage of online resources and participate fully in modern society, must be balanced against the potential risks outlined above, regulators will need to emphasise skill development, education and information sharing as key aspects of any regulatory infrastructure.

In addition, the development of a self-regulatory system, such as the *Safer Social Networking Principles for the EU*, would provide a useful baseline of practice for SNS providers, against which their dealings with users, including young people, could be assessed.

Lessons to be learnt from the studies and the regulatory responses to date include:

- The adoption of an approach based on appropriately managing risks, not inhibiting use.
- Any policy response to the problems arising from the risks of using SNS must involve multiple stakeholders, including governments, SNS operators, parents, teachers and students. The US Joint Statement on Key Principles of Social Networking Safety and the EU Safer Social Networking Principles provide good examples of processes that engage SNS service providers in working towards best practices.
- There is no ‘one size fits all’ regulatory response.
- Any regulation must incorporate a combination of modalities, including education, technologies, self-regulatory codes, and policies implemented through SNS terms of use.
- To date, police responses to risks associated with SNS use in all jurisdictions studied for this report have tended to be fragmented and insufficiently coordinated.
7. Conclusion

This chapter of the report summarises the research findings of the project and sets out recommendations arising from those findings. While considerable care has been taken in compiling the research data and assessing the findings, some caution is naturally required in drawing broad conclusions from what remains a single, preliminary study. Nevertheless, we believe that the findings are sufficiently robust for us to make some significant recommendations concerning the legal risks facing young people in the use of SNS, and the appropriate policy responses to those risks.

7.1. Research findings

The research undertaken for this project revealed the following about SNS usage by Victorian middle school students:

1. The overwhelming majority of middle school students surveyed have used SNS, with 94.9% of surveyed students reporting use of at least one SNS.
2. Teachers and parents of middle school students are generally well-informed regarding the extent of use of SNS by middle school students.
3. There are generally few gendered differences in the use of SNS by middle school students, although a larger percentage of female students use SNS to stay in contact with ‘friends’. While male students are more likely to post photos to a friend’s page than females, female students are more likely to send private messages to friends.
4. Middle school students are not necessarily aware that information about themselves placed on a SNS can constitute a profile.
5. Facebook is far and away the most popular SNS, with 93.4% of students using it, followed by MySpace, with 26.6% of surveyed students using it. Many students use more than one SNS.
6. The most significant factor in determining the choice of SNS was peer influence, with 45% of surveyed students indicating that their friends were a significant factor in determining choice.
7. There is a relatively high frequency of use of SNS, with the majority of surveyed students updating information on their SNS at least on a daily basis, and over a quarter updating their SNS profile several times a day.
8. While the majority of surveyed students affirmed that SNS is important to them (60.3%), only 33.4% were strongly affirmative about the use of SNS. Most of the responses which provided detail either suggested the students saw SNS as a useful communication tool, or for stimulation when ‘bored’.
9. Although there was generally a decrease in the perceived importance of SNS with age, this was not reflected in any change in the frequency of students updating their SNS.
10. Overall, students indicated that they used SNS to communicate with current friends and especially to stay in touch with friends they rarely see in person. The surveyed students use SNS primarily to maintain current social networks, while making new friends and flirting were relatively low in students’ reported practices.
11. While some parents communicate with their children using SNS, over half did not do so. Nevertheless, the majority of parents (80.4%) indicated that they had seen their child’s SNS profile.

12. The most common content reported as posted to SNS by surveyed students is photographs of themselves (60.9%), closely followed by photographs of their friends (52.6%). Nevertheless, posting of third party content, including music, video and photos of celebrities, is still significant. The proportion of students posting videos to SNS increases with age.

13. Importantly, a significant proportion of students (45.6%) reported that their photos had been posted on their friends’ SNS. In addition, a majority (62.1%) reported that photos of their friends had been posted on other people’s SNS.

14. Despite the prevalence of practices involving the ‘sharing’ or posting of photographs depicting students, the vast majority (80.3%) were not concerned with this, with 19.7% reporting that they were concerned.

15. While a majority of middle school students (67.6%) believed that their SNS is an exact or partial reflection of themselves, a proportion (11.3%) indicated that it showed an idealised version of themselves. A proportion of students are aware of mixing elements of truth and fiction in their SNS profiles.

16. The most highly valued feature of SNS was the ability to stay in touch with friends and family (49% of respondents). SNS are also perceived to be less expensive than other forms of communication. A minority of students (3.3%) indicated that SNS enabled them to expand their social network.

17. The majority of teachers surveyed were favourably disposed to the use of SNS by students, with 48.8% indicating that SNS are beneficial for keeping in touch with people, while 19.7% indicating that there were benefits to the school and for pedagogical activities in SNS use. On the other hand, a strong minority (37.8%) indicated that they felt there were no benefits for students using SNS.

18. While the majority of parents (77.6%) reported some degree of support for, or ambivalence towards, their children using SNS. The remaining 22.4% of parents indicated they were not aware of any benefits, with some expressing concerns.

19. Surveyed students felt that SNS were safer than did their teachers and parents. Thus, while 48.8% of students recognised that there was some element of risk in using SNS, more than one quarter (28.3%) thought that SNS were safe. Moreover, 19.6% of students were ambivalent about risk, essentially reporting that the degree of risk was irrelevant to them as it is “just what everyone does”. There is an apparent decrease in age with the perception of an element of risk in SNS usage, with a corresponding increase in disregard for risk. Female students were slightly more inclined to perceive SNS as risky.

20. Students from years 7 to 10 are increasingly more selective in who can see their profile. The survey results suggest that year 7 students not only have more visible profiles, but are more likely to perceive SNS as safe or only a little bit risky.

21. While a significant minority of surveyed students (21.7%) appear to be either unaware of, or unconcerned about, potential risks in using SNS, a majority of students (61.3%) reported potential risks from unwanted attention from others or cyber-bullying. Both of these concerns reflect popular concerns of media and government.

22. A majority of surveyed students (72.4%) indicated that they had had unwanted or unpleasant contact by strangers via their social networking profile. A minority of
students (13.8%) were concerned about security risks relating to their, such as identity theft. A relatively small group of student respondents (3.2%) identified concerns relating to privacy or unwelcome disclosure of data.

23. Teachers were particularly concerned with issues of cyber-bullying (43.6%), and grooming or stalking (27%), with a lesser number (14.2%) expressing concerns about identity theft.

24. Parents, like teachers were concerned with cyber-bullying (22.4%) and grooming or stalking (12.2%), while they were also concerned about risks to privacy in the form of disclosure of personal information (14.3%).

25. Despite the acknowledged risks of students using SNS, there is surprisingly little ongoing conversation about SNS use between parents and their children, on the one hand, or teachers and their students, on the other. In this respect, almost half of the surveyed students (46.1%) reported that they did not talk with their parents about SNS use, while almost three quarters of the students (74.6%) reported that they did not talk with their teachers about SNS use. A common explanation given by students for the lack of communication with teachers was that they felt teachers were not experienced enough to talk about the risks of SNS.

26. While a majority of students reported that they did not discuss the risks of using SNS with their teachers, the majority of teachers surveyed (68.6%) reported that they had discussed SNS risks with their students. Further research is needed to resolve this apparent discrepancy. Although most teachers reported raising the issue with students, there were also some concerns about the lack of time in a crowded curriculum to seriously address the risks of using SNS.

27. While most parents reported that they talked to their children about the risks of SNS, many indicated that their children were reluctant to listen or dismissed concerns.

28. A majority of surveyed students reported that a stranger had contacted them in an unwelcome or unpleasant way via SNS. The majority of students who had been contacted appear to have adopted simple strategies for dealing with this contact. Thus, 43.4% reported that they either deleted or blocked the contact, while a further 15% reported that they ignored the contact. Nevertheless, none of the students who reported an unwelcome contact indicated that they had informed an adult, notified the SNS service provider, or reviewed their security settings.

29. Surveyed students reported an awareness of a variety of strategies for avoiding risks or problems associated with SNS use, including ignoring ‘friendship’ requests from strangers, blocking or deleting unpleasant or unwanted friends, setting their profile to ‘private’, not disclosing personal details, frequently changing their password, threatening people who wished to be added to the student’s SNS and self-censorship. Only 1% of respondents reported asking for guidance or help from adults as a viable strategy.

30. A number of the students interviewed indicated that they protected their privacy by withholding information, or providing inaccurate information, on their SNS.

31. A majority of teachers surveyed on the issue (68.5%) reported that they used a SNS. While 37.7% of this group reported relatively low privacy settings, 62.3% were selective about who could access their SNS profile.

32. Of the teachers surveyed on the issue, 63.9% reported that they had not used SNS in an educational context. Nevertheless, a significant minority (36.1%) of the teachers
who were asked this question indicated that they had used SNS for educational purposes, including communicating with their students about schoolwork.

33. The majority of teachers who were surveyed on the issue indicated that they were aware of risks, including legal risks, of teachers using SNS. A majority (82.4%) expressed a range of concerns relating to defamation, disclosure and privacy, although none expressed concerns about breaches of copyright.

34. The great majority of teachers surveyed on these issues (81.3%) expressed concerns that, due to the informality of SNS use, and the associated potential to share too much information, using SNS to contact students risks compromising their professionalism, and can raise issues related to a teacher’s duty of care. In all, 27.5% of teachers surveyed on this issue made non-specific statements about risks associated with their duty of care. Moreover, 29.9% were specifically concerned with legal issues arising for teachers as a result of inappropriate information being discovered on students’ SNS sites, which could give rise to professional or legal obligations.

35. A significant minority of teachers surveyed on this issue (24.1%) were concerned about students finding out information about the teacher via a SNS, and the attendant loss of privacy, which could negatively impact on the professional relationship between teachers and students.

7.2. Recommendations

The research findings of this project confirm that SNS usage is now playing an important role in the lives of Victorian middle school students, including in socialisation and identity formation. In fact, SNS use has become integrated into the everyday social lives of most Victorian middle school students.

In general, our results indicate that there is a general degree of awareness of risks in using SNS by middle school students, although concerns about risks differ markedly between parents and teachers, on the one hand, and students, on the other. The research findings also indicate that there is a high degree of trial and error in how middle school students are seeking to manage risks associated with SNS use. Moreover, although there is some degree of understanding of legal risks, there is very little clear understanding by students, parents and teachers alike, of the precise nature of the legal risks that may arise from everyday SNS use. On the other hand, there is much more awareness of the more dramatic and impactful risks associated with cyber-bullying, or grooming and stalking.

Given the findings of this preliminary study reported above, and in the context of the ongoing significance of SNS use among middle school students, the key recommendations arising from this project are as follows:

1. In order to enhance the benefits of SNS use, and minimise the disadvantages, it is important for children and young people to be equipped with the necessary information to empower them to effectively manage risks associated with the everyday use of SNS. The best way to do this is through specifically tailored educational activities. As children and young people must be primarily responsible for managing their own risks, it is essential that educational activities focus on providing clear and accurate information about all risks associated with SNS use, including legal risks. These educational activities should be aimed primarily at equipping children and young people with the skills required to be effective digital citizens, and not focussed on rare or hypothetical fears.
2. Education about the full range of legal risks potentially encountered by the use of SNS should be part of a fully integrated cybersafety school curricula. This means that attention that is properly given to more dramatic issues, such as cyber-bullying and ‘sexting’, should be balanced with attention to other potential areas of legal liability. This strategy should also assist in promoting awareness of, and debates about, the Australian legal system as it applies to online activities. While acknowledging the crowded nature of school curricula, the importance of SNS in the lives of students, and the potential significance of social media for future digital citizenship, suggests that room should be found for these issues to be directly addressed.

3. The best way to approach the teaching of legal literacy in the digital environment, is by the use of practical examples drawn from real life case studies. With this objective in view, one of the outcomes of this project is the Education Resource Book, which includes a series of classroom exercises aimed at promoting understanding and discussion of specific legal issues. The researchers for this project encourage the production and use of this and similar resource material for the use of teachers of middle school students.

4. The reported prevalence of posting of photographs of students to SNS, suggests that the legal and ethical issues involved with the posting of photographs – which include privacy, confidentiality, defamation and copyright – merit specific attention in any cybersafety curriculum. The significance of understanding these issues is emphasised by the incidents involving a Melbourne teenager posting naked photos of AFL footballers to her Facebook site.

5. The potential disparities in the approaches to, and understandings of, legal risks associated with SNS use between parents, teachers and students, as well as the reported paucity of communication on SNS use between students and parents and teachers, suggests that there is some need for education and training of teachers and parents, as well as students. Much can be gained by the community from greater informed discussion of the implications of SNS use, including legal implications, among parents, teachers and students.

6. Consideration should be given by Commonwealth, State and Territory authorities to encourage and guide SNS service providers operating in Australia to enter into a self-regulatory agreement similar to the Safer Social Networking Principles for the EU. This would provide baseline commitments against which practices of SNS service providers in their dealings with young people could be periodically assessed.

7. Given the concerns expressed by teachers interviewed for this project, there appears to be an identified need for further guidance to be provided to teachers about the use of SNS, especially in the pedagogical context. In particular, there is a pressing need for research and policy work to be undertaken in determining the extent of the ‘duty of care’ owed by teachers in any interactions with students via SNS. In this respect, it is important that the salient differences between interactions via SNS, and interactions offline, including the different legal implications, are fully taken into account.

8. There is a need to promote holistic policy responses to the full range of risks associated with the use of SNS by young people. Any responses should be coordinated so as to minimize the risk of fragmented, inconsistent, and potentially contradictory, policy initiatives at the Commonwealth, State and Territory levels. If, following the forthcoming report by the Commonwealth Joint Select Committee on Cyber-Safety, it is decided to establish an Online Ombudsman, the Ombudsman’s portfolio should extend to promoting education about the full range of legal risks associated with the
use of SNS. In doing so, the Ombudsman should coordinate with Commonwealth, State and Territory Privacy Commissioners.

As the discussion of the project above indicates, this was a preliminary study, which, as well as highlighting the issues analysed above, also indicated the need for further work to be done in this area. There is a need for further research directed at understanding young people’s use of SNS and how they can better be empowered to be confident and safer digital citizens. There is also a significant need to further work to be done to assist teachers to be better equipped to understand their rights and responsibilities in the digital communication environment.
8. Bibliography


[107]


