SUBMISSION No. 98

Submission to Joint Select Committee on Cyber-Safety

by the

Office for Youth (South Australia)

9 July 2010

Overview

This submission has been prepared by the South Australian Office for Youth and draws on data collected through the Office for Youth's recent Social Networking Education and Awareness Campaign about the risks of using social networking.

This submission also includes comments from the following agencies:

- Office of the Guardian for Children and Young People (GCYP)
- Department for Families and Communities (DFC)

The submission relates to the Terms of Reference 1, 2, 3, 4 and 5.

Contact Officer:
Suellen Priest, Policy Officer, Office for Youth
Level 5, 11 Waymouth Street, Adelaide SA 5001
(08) 8204 8462

Background

The Office for Youth recently ran a Social Networking Education and Awareness Campaign in response to a growing concern about the risks to young people associated with using social networking sites. The key initiatives were a Safer Social Networking two day info-line, an online survey, and a one-stop-shop Cyber Safety Information Portal.

The temporary **Safer Social Networking info-line** ran from 4pm – 11pm on Wednesday 16 and Thursday 17 June with the aim of connecting young people and their parents with the necessary information to enable them to better understand, and set, privacy settings on their social networking site and to identify key issues for young people relating to social networking.

The **online survey** was placed on the Office for Youth website to identify the key issues associated with social networking.

The **one-stop-shop Cyber Safety Information Portal** provides young people and their parents/carers with a range of information on cyber safety through one entry point on the Office for Youth website.

Twenty-seven people called the info-line and 103 people responded to the Office for Youth's survey. These initiatives have identified a range of issues that are relevant to the Join Select Committee's Terms of Reference. These issues are outlined in this submission. Please see Attachment 1 for a full list of the issues identified through the campaign.

General comments

With regard to the Joint Select Committee on Cyber-Safety's Terms of Reference, the Office for Youth recommends that the committee note the following:

1. Children and young people have the right to freedom of expression and use of available technologies, when it is safe for them to do so.

2. Online social networking provides many benefits to children and young people such as:
    - the creation of online media content (rather than just consumption)
    - the social rather than solo nature of internet discovery
    - discovering new experiences (music etc)
    - getting peer support for personal issues
    - the ability to take part in groups with similar interests (school, music, film etc)
    - keeping in contact with real world friends
    - providing a platform for self-expression
    - meeting new people online from around the world
    - more cost-effective to chat online than make mobile or long-distance phone calls
    - relieving boredom.

3. Engaging with children and young people about new technologies is a constructive parenting and educative role, particularly in talking about safety and wellbeing.

It is therefore important that the risks of new technologies and social networking are addressed in a positive and enabling way, for example:

- For the community – that children and young people have rights to expression, privacy and to be free from bullying
- For parents – how to intervene positively but decisively if things seem or feel unsafe
- For children and young people – how to make smarter choices
- For schools and other child or youth settings – safe use and counter-bullying strategies

Comments on the Terms of Reference

Term of Reference (1) "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)"

- In relation to '*stakeholders controlling or able to influence that engagement*', the following should be considered:
    - are there issues with government and non-government agencies engaging vulnerable young people through social networking and social media
    - youth worker or case worker being a 'friend' of a client on Facebook
    - the capacity of employees to engage with young people professionally and safely to ensure the young person receives the maximum benefit
    - any issues arising regarding mandatory reporting or other legislative requirements

- With social networking and internet use among young people set to continue to increase, government employees and service providers will use these tools to engage with young

people, particularly vulnerable young people. Sound policy and associated guidelines, in addition to education and awareness will be important in managing these issues.

Term of Reference (2) "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"

- In terms of online cyber-safety threats, the Office for Youth's Social Networking Education and Awareness Campaign showed public concern about a number of online safety issues, including: underage users, cyber bullying, victimisation, stalking, slander, hacking, young people trusting people without knowing who they really are, identity theft, fraud and the fact that it is too easy to lie about identity online.

- The Social Networking Education and Awareness Campaign also recorded a large number of concerns about the level of access others have to their information (or their children's information). These concerns included: over-sharing of person information, third party access to your information, apathy around setting privacy settings, lack of information about how young peoples' information can be used for identify theft, young people too trusting and accepting anyone as a friend, pressure to 'collect' friends and have lots of friends to fit in – giving a large number of people access to their information. There is also concern about people posting images of other people without consent and stealing photos and online content.

- In relation to this Term of Reference, the Office for Youth recommends:

    - That the additional cyber-safety threats outlined above are considered in this term of reference.

    - That the level of access to information, and the privacy and safety risks associated with this, is considered as an area of investigation.

    - That the committee particularly consider the risks associated with children under 13 using social networking sites such as Facebook where they must lie about their age in order to have an account (this means that Facebook accepts no responsibility for these young users).

    - That the committee particularly consider breaches of privacy in relation to social networking sites such as Facebook.

Term of Reference (3) "Australian and international responses to current cyber-safety threats (education, filtering, regulation, enforcement) their effectiveness and costs to stakeholders, including business"

- In relation to Australian responses to current cyber-safety threats the Office of the Guardian for Children and Young People (GCYP) suggests:

    - That service providers (e.g. Facebook) be obligated to provide easy and default methods of protecting privacy for children and young people.

    - That there is easy access to advice and resolution of complaints for parents and young people.

- The Social Networking Education and Awareness Campaign showed that people feel there needs to be more education and information about the risks of online activity. Additionally, those who had experienced a cyber-safety threat did not feel that their concerns were adequately addressed. Respondents identified concerns about education and enforcement as outlined below:

    - **More education**
      Respondents to the Office for Youth's safe social networking survey and info-line indicated that more education is required, particularly around the following areas: knowing what to do if something happens to you online; understanding your rights as a user; understanding that same social rules and laws apply on-line as in the 'real world'; what parents/grandparents/caregivers can do if they are concerned about their children's safety.

    - **Enforcement**
      The Office for Youth two-day info-line referred thirteen callers to the police or Australian Communications and Media Authority (ACMA) to investigate cyber-safety threats. Many of these callers had already spoken to the police and felt their concerns had not been adequately responded to. Other callers who rang in with a cyber concern (cyberbullying, hate Facebook pages etc.) did not know who to contact for assistance and there is no clear agency responding to cyber-safety threats, particularly for young people.

- In relation to this Term of Reference, the Office for Youth recommends the scope be expanded to also consider gaps in Australian responses to current cyber-threats.

Term of Reference (4) "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"

- The Office for Youth's Social Networking Education and Awareness Campaign showed that many people are concerned about cyber-bullying and have had negative experiences online.

- Additionally, the Office for Youth's recent Judge Hora A-Team (Action Team)[1] recommended that schools adopt restorative practices, the 'use of a structured discussion process between students or adults to resolve conflict, address harm caused, and agree to a way forward'[2], as a way of managing bullying incidents better. These practices would also be applicable to cyber bullying incidents, particularly around changing the culture of schools.

[1] A-Teams are an Office for Youth initiative run in partnership with Adelaide's Thinkers in Residence. The initiative brings together a team of young people aged 16 to 25 years to work with the current Thinker in Residence and develop recommendations for government and the community relating to the Thinker's residency. The Judge Hora A-Team worked with Thinker, Judge Peggy Fulton Hora (Ret), and examined the topics: appropriate dispute resolution in schools and ways to improve public confidence in the courts.

[2] Behaviour4learning, Restorative Approaches, viewed June 2010 at http://www.behaviour4learning.ac.uk/ViewArticle2.aspx?startchar=Q&endchar=T&menu=10127&ContentId=10540

- In relation to this Term of Reference, the Office for Youth recommends:

    - Clarifying who has responsibility for responding to cyber bullying issues (for example, schools or police) and the development of clear policies for responding to cyber bullying.

    - Consideration of restorative practices as a method of responding to cyber-bullying and changing the culture of schools.

    - Empowering children and young people by, for example, teaching them about appropriate assertive responses, how to make wise choices when they feel uncertain, and not to panic when there is a problem but talking about it with the appropriate authorities.

Term of Reference (5) "the merit of establishing an Online Ombudsman to investigate, advocate and act on cyber-safety issues"

- The Office for Youth is very supportive of this Term of Reference. As mentioned above, there is no clear agency responding to cyber-safety issues and quite a bit of public confusion about who to go to for help. Additionally, there is public concern that police responses are not always adequate and often when people do seek help, there is little that can be done and the individual is left feeling frustrated that there is no one to follow up and resolve their concerns.

Attachment 1 – Responses to the Office for Youth's Social Networking Survey - 2010

Identified issue of concern	%	No. of responses
Access to personal information (i.e. over-sharing of person information, 3rd party access to your information, apathy around setting privacy settings, lack of information about how your person information can be used for identify theft, fraud, young people too trusting and accept anyone as a friend, there is pressure to 'collect' friends and have lots of friends to fit in – giving lots of people access to their information.)	25.1	62
Personal safety (i.e. cyber bullying, victimization, stalking, slander, hacking, trusting people without knowing who they really are, identity theft, fraud, too easy to lie about identity, concern that police response not adequate)	21.1	52
Education/Awareness (i.e. not knowing what to do if something happens, lack of understanding of your rights as a user, lack of understanding that same social rules and laws apply on-line as in the real world, parents/grandparents concerned about their children's safety but don't know what to do about it)	13.4	33
Cyber bullying and harassment	12.1	30
Inappropriate contact/content (i.e. information posted about you without your knowledge/permission, parents posting photos of their young children, young people posting inappropriate information about themselves, vulnerable young people more at risk, general perception that it's on the internet therefore it's true, pressure to accept friend requests from strangers/people you don't like)	10.1	25
People posting photos of others without permission (i.e. people putting up photos of friends, family or others without asking or informing them, people stealing other's photos)	6.1	15
Social networking privacy settings (i.e. not aware of them, not knowing how to set them, default settings too open, personal info not protected, should have to set up privacy settings – shouldn't be optional)	5.3	13
Young people unaware of the consequences of posting online and the permanence of that information (i.e. lack of understanding about what happens to information you post online, and how it's online forever)	4.0	10
Underage use (i.e. under 13's lying about their age to set up a profile, mixing of young people with adults in nonsupervised setting)	2.8	7
Total	**100**	**247**

Source: SA Office for Youth's 2010 Social Networking Survey