

E-Safety and Web2.0 for children aged 11-16

Mike Sharples^{*}, Rebecca Graber^{*}, Colin Harrison^{*}, Kit Logan[#]

^{*}Learning Sciences Research Institute, University of Nottingham

[#]London Knowledge Lab, Institute of Education, London

Abstract

A central challenge for schools in considering the adoption of social network and creative media (Web 2.0) technologies is how to support children to engage in productive and creative social learning while protecting them from undue risks. This paper reports findings from a survey and interviews with children aged 11-16, teachers and parents on their attitudes to e-safety and their practices at school and at home. The results showed that 74% of the children surveyed have used social network sites and that a substantial minority regularly interact socially online with people they have not met face to face. Online interaction forms a different, though overlapping, social space to that of face to face friendships.

Despite a desire from some teachers to explore the benefits of Web 2.0 for creative and social learning, they report being constrained by a need to show a duty of care that avoids worst case risk to children, to restrict access to social network sites. The respondents also report more direct concerns about internet bullying and exam cheating. We also report a Policy Delphi process with a panel of 30 people with expertise in Web 2.0 and e-safety, to propose, elaborate and then rank 'positions' (informed defensible viewpoints) on e-safety for their desirability and feasibility of implementation. The Delphi panel reached a general consensus that schools should move towards allowing access to Web 2.0 sites, with children being educated in responsible and creative learning.

Background

The worldwide web can offer learning opportunities for people of all ages. It is a rich and rewarding source of knowledge and a medium that empowers creativity and imagination. Interacting with social network and media sharing sites such as Facebook, Bebo, MySpace and YouTube (which for convenience in this paper we shall refer to as Web 2.0 (O'Reilly, 2005)) also presents particular risks to young people, including exposure to online bullying, inappropriate material, possibility of contact with harmful strangers and opportunities to cause harm to others. A central dilemma that schools must address in a consideration of e-safety and Web 2.0 activity is how they can support children to engage in productive and creative social learning through web technologies while protecting them from undue harm.

There is no simple or mechanistic solution to this dilemma, since creativity and social interaction necessarily involve an element of risk, in exposing oneself and one's ideas to criticism and possible abuse. In a search for a philosophical and political framework, we could turn to the United Nations Convention on the Rights of the Child (United Nations, 1990). Article 13 declares that "The child shall have the right

to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.” It then indicates that the exercise of these rights may be subject to certain restrictions, “but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; or b) For the protection of national security or of public order (*ordre public*), or of public health or morals”. So, we again face the problem of how to allow children the right to freedom of expression in the media of their choice, while ensuring appropriate protection of their health and morals.

Underlying this is a moral and ideological difference between those who see a primary role of adults as being to nurture children and protect them from harm and those who wish to liberate children to express their natural curiosity and creativity. At the extremes, these ideals are clearly incompatible; however, philosophers of education from Rousseau onwards have proposed the creation of ‘walled gardens’ where children should be enabled to express themselves freely within a safe and supportive environment. Whether such protected educational spaces within the Internet are compatible with the ethos of Web 2.0, whether they foster appropriate education for life, and whether they will be welcomed or dismissed by children, are central to the development of policy for social networking in education. To investigate further, we shall need to unpack the elements of e-safety and Web 2.0, in order to understand current practices and fears, and to propose some reasoned approaches.

The paper begins with a review of literature on the benefits and risks to teenage children of Web 2.0 activities. It then reports results of a survey of 2611 children and 206 teachers from 27 schools across England, plus 121 parents of teenage children. The survey data were supplemented with focus group interviews with students at 25 schools and individual interviews with approximately 150 teachers, managers and technical staff to form a rich picture of web 2.0 activities and concerns. The project also commissioned an Advisory Panel of thirty people with expertise in e-safety and creative use of web technology. The paper reports the process and outcomes of a Policy Delphi study with this panel, to propose, critique and rank policy options related to e-safety and Web 2.0. A concluding section discusses the difficulties for schools and society in developing policy that supports children in creativity and learning through the social internet while exercising a duty of care.

Society’s fears

For over half a century, adults have sought to protect children from the perceived dangers of new media. A substantial report published by UNSECO in 1953 (Bauchard, 1953) discussed the effects of press, film and radio on children, including the harmful effects of popular song lyrics. In relation to the new medium of television the report states “that problems will arise there can be no doubt” since television shares with radio the power of entering the home everyday and is “exercised at once on the eye and the ear. It therefore seems likely that the problems of television for children will make themselves felt with even greater urgency than has been the case with these other media of expression.” The report cites evidence that children in some parts of the US spend nearly four hours watching television, “which means that they spend more time watching television than they do in school.”

The language of the 1953 UNESCO report is strikingly similar to the recent report of the Byron Review on 'Safer Children in a Digital World' (Byron, 2007). Both warn against the encroachment of a new medium (television, the internet) into children's lives; they criticise sensational accounts of the dangers but are concerned about what children might learn from the new medium and how they will be influenced; they both call for further monitoring and protected areas where children can engage with child-appropriate content while recognising that children will continue to explore the adult world; and they demand further research into the effects of the medium on children's wellbeing.

It would appear that a new mass medium becomes an emblem for society's unease about modernity. That children so readily adopt the medium and make it their own, showing an ease with the technology and developing a culture that excludes adults, is seen as provocative and unsafe. Led by press coverage of children being led astray, the new medium is cast as a threat to childhood, a problem to be solved. Recurring themes are the threat to traditional education ("they spend more time watching television than they do in school"), inappropriate contact with adults (now reduced to the catchphrase "stranger danger"), provocation to violence, and precocious behaviour.

The Byron review has been influential in raising considerations of e-safety amongst policy makers and the public, yet even to start with a consideration of risk is to make a value judgement. Although the Byron Review mentions the value to children of internet use, the Review was only commissioned to make an assessment of risk, not benefit.

Benefits of Web 2.0 activity

Safe internet use requires balancing perceived benefits against acceptable risks. Green and Hannon (2007) have indicated benefits to young people from engaging in online social networking, including the development of skills required to prosper in the 21st century such as creativity, ideas generation, presentation, leadership, team-building, confidence, communication, innovation, initiative, critical awareness in information gathering, and ability to evaluate, question and prioritise information. Children can gain confidence from creating and managing an online persona, from publishing online and gaining approval, and from developing hobbies with like-minded people. No matter how specialised your interests, there is always someone on the web to share them.

Green and Hannon (2007) propose that digital technologies offer a 'third space' between formal and informal contexts, where young people can create portfolios of digital media, engage in peer teaching, and develop their confidence and voice. Such activities are ingrained into the lives of young people, through their engagement with media sites and online games. As the authors indicate, none of these 'soft skills' are explicitly taught in schools. "In fact the idea that they can be taught in any traditional sense with a teacher standing at the front of a classroom is disputable." (Green and Hannon, 2007, p. 23)

While children can gain valuable skills by engaging in the activity of online social networking and new media creation, without any need for formal teaching, there are also opportunities to apply these skills and technologies to school education. Companion papers from the Becta project 'Web 2.0 Technologies for Learning at Key Stages 3 and 4' will be published that indicate how Web 2.0 technologies are being adopted in UK schools. A main finding from that project is that restrictions on children's access to social networking sites have meant that very few schools have, so far, explored their value for learning. Pioneering projects have included: using blogs to encourage debate amongst students; a combination of podcasts and a blog by a music department to comment on performances; the use of a wiki for students to collectively develop a set of 'class rules' for the computer room; employing forums to support research and knowledge sharing in English and Media Studies; and social bookmarking for sharing of online resources.

In many ways, the early use of these tools in school has been similar to that in universities, to encourage critical debate and support collaborative research. The results are similar to those reported amongst university students, including successful knowledge sharing, social cohesion, and a wider range of contributions than in class discussions (Wright & Lawson, 2004). For example, one Media Studies teacher interviewed for the Becta project who had used online forums for critical discussion of Hitchcock commented that every child from a class of thirty had contributed, with boys and girls who would not normally talk to each other in class posting questions to each other and praising each other's contributions. Wright and Lawson (2004) indicate that student engagement in online group learning activities is strongly predictive of higher academic achievement, but this has still to be tested in schools. Computer-supported collaborative and creative learning is being explored by a few pioneer schools, but for this to be adopted more widely requires not only access to the tools for social networking, but also the development of methods of teaching and assessment that value creativity, teamwork and peer teaching.

Risks of Web 2.0 activity

To assess the risks of Web 2.0 activity, it is important to separate them from societal fears. The fears relate to children being exposed to inappropriate content, children being abused by strangers, and online bullying (Byron, 2007, p. 4). What is the evidence that these pose real risks to children?

Inappropriate content

Inappropriate content ranges from advertising (e.g., for fattening foods and sweet drinks) to portrayals of violence and pornography in websites that children can access. The Byron Review has addressed risks to children from exposure to potentially harmful or inappropriate material on the internet and in video games. Delivery of web content is not a focus of Web 2.0, so we shall avoid covering the same ground. It is difficult territory to negotiate, given changing views on what is and is not appropriate for children see at different stages of their development.

Abuse of children

By contrast, the abuse of children by adults through the Internet is facilitated by the social internet. Adults can assume false identities online, pose as young people and hide behind a cloak of anonymity. The Byron Report claims that 'stranger danger' is

“one of the greatest risks related to contact on the internet” (Byron, 2007, p. 53). It cites the report of the UK independent regulator of communications industries (Ofcom, 2007) in saying that “Adults masquerading as younger people is one of the biggest issues parents say they are most concerned about with the internet.” (Byron, 2007, p.53). This phrase ‘stranger danger’ taps a deep-rooted fear in parents of their child being abducted or abused, a fear exploited by media reports of online predators stalking internet chatrooms.

Here, we must distinguish between likely risk and worst case risk. The risk of children being duped by online predators is extremely small. An extensive study of internet abuse cases in the United States (Wolak et al., 2008) concludes that “the publicity about online ‘predators’ who prey on naïve children using trickery and violence is largely inaccurate” (Wolak et al., 2008, p. 111). The report indicates that the reality about Internet-initiated sex crimes – in which sex offenders meet juvenile victims online – is different, more complex, and serious but less archetypically frightening than the headlines suggest. The internet may make youths more accessible to offenders and create opportunities for molesters to be alone with victims (Wolak et al., 2008, p. 121). In most cases, though, the victims are aware they are conversing online with adults and offenders rarely deceive victims about their sexual interests. Most victims who meet offenders face to face go to such meetings expecting to engage in sexual activity. “Most offenders are charged with crimes, such as statutory rape, that involve nonforcible sexual activity with victims who are too young to consent to sexual intercourse with adults.” (Wolak et al., 2008, p. 113)

Inevitably, such ‘worst case scenarios’ are promoted by media eager to report incidents of criminality and excess, but where such incidents have occurred, or could occur, then they provide the impetus for policy. In an increasingly risk-averse society, where schools and Local Authorities are vulnerable to legal action by parents, there is a strong incentive to try and prevent worst case risk to children within the purview of schools.

In the case of Internet activity, this often means preventing children from engaging in any social activity on the Web at school and tightly controlling the websites that they can access. Yet, while this may remove the immediate danger to children and protect the school or Local Authority against lawsuits, it may also store up further problems. As with any prohibition, children become expert at finding ways round it, aided by the many websites offering techniques for ‘backdoor access’ to forbidden content and services.

Cassell and Cramer (2007) advance an argument that young women have been both empowered and constrained throughout the history of communications technology, from the telegraph onwards. Like Wolak et al. they offer evidence that the dangers to girls online are not as great as have been portrayed in the media, and argue that concerns about internet predators have arisen from adult fears about girls’ sexual agency. New communications technologies enable young women to socialise online, leading to an increasing confidence with technology and also to their displaying aspects of adolescence, including behaving in sexual ways. Parents, not understanding this new familiarity with technology and concerned about their children moving outside control, become afraid for their safety. This creates a ‘moral panic’, inflamed by a prurient press, that restricts girls’ use of technology and keeps them within an

adult sphere of control. The result is that girls are prevented from exercising their creative and social power in the new medium.

Clearly, e-safety is a social and political minefield. It may help in exploring the difficulties to re-fashion the central dilemma into a set of operational choices relevant to Web 2.0. Should schools and local authorities guard against the worst that may happen when children socialise on the internet, or should they develop policy based on continually assessed levels of acceptable risk? Should schools be places apart from online social networking, or do they have a responsibility to help children develop appropriate skills for engaging with the new Internet?

To make such choices, schools need to look beyond current preoccupations to the underlying issues and risks. Thus, there is currently much concern that posting personal information on social network sites such as Facebook, MySpace and Bebo is putting children at risk of abuse. The research by Wolak and colleagues indicate that “posting personal information online does not, by itself, appear to be a particularly risky behaviour” (Wolak et al., 2008, p. 113). Youths who created personal profiles or posted photos of themselves online were more likely to get contacts from unknown people, but were not more likely to get contacts that they described as scary or uncomfortable. The researchers found no empirical evidence that just posting personal information exposes young people to online molesters or stalkers, but certain types of online behaviour may make youths vulnerable. These included interacting online with unknown people, having unknown people on a friends list, chatting online about sex, seeking pornography, and being rude or nasty. The authors emphasise that the research data is still scarce and so should be treated with caution. “There may be risks associated with posting particular kinds of information or posting in particular venues that research has not discerned.” (Wolak et al., 2008, p. 117)

One conclusion from this research is that just preventing children from joining their peers in the normal behaviour of social networking, including posting some personal details, may stoke up resentment, leading to subversive behaviour. A more subtle approach is needed to distinguish between activities with higher and lower risk. It may be more effective to educate children to appreciate when they cross the line from acceptable to abnormal and risky Web 2.0 activity. Schools could provide such guidance, but only if they understand the norms, habits and risks of social networking.

Online bullying

Bullying online, or cyberbullying, can be an upsetting experience. A survey by Li (2006) of 264 students from three junior high schools in Canada showed that almost half of the students were bully victims and about one in four had been cyberbullied. This percentage matched that from a smaller study conducted in London (though this included phone calls and text messages) (Smith et al., 2006). The Canadian study showed no significant difference between the proportion of male and female students who reported being bullied. The London study showed that phone call, text messages and email were the most common forms of cyberbullying, while chat room bullying was the least common. It showed that girls were significantly more likely to be cyberbullied than boys, especially by text messages and phone calls. A recent phenomenon is posting hurtful images and videos on the web. Children can write abusive messages on discussion boards and contribute to websites that criticise their teachers and schools.

Cheating online

At the other end of the 'fear' spectrum from child abuse is cheating online. Children are empowered by Web 2.0 technologies to copy, share and paste materials in ways that may be seen as cheating within the school system of teaching and assessment, even if the children do not regard their activity as such. They can communicate by text messages within the classroom and increasingly, they are able to access the web through a mobile phone. This is a grey area of school discipline. Most schools officially ban children from bringing mobile phones into classes, yet many teachers accept that children carry mobile phones and that some parents insist on this, for their children to contact them in an emergency. For some schools, accessing a Web proxy site (a means to access banned websites) is a disciplinary offence; in other schools it is accepted or even encouraged by teachers as a means to by-pass Local Authority restrictions that prevent access to educational resources. The challenge for schools is to enable children to develop essential skills of digital and media literacy, including personal media creation and critical understanding of computer media, while making clear the boundaries between creativity and plagiarism or collusion.

Survey and interview findings related to e-safety

The University of Nottingham, in partnership with the London Knowledge Lab and Manchester Metropolitan University has been commissioned by Becta (the agency responsible for strategic development and delivery of the UK Government's information and communications technology (ICT) and education strategy) to undertake a review of Web 2.0 technologies for teaching and learning by children aged 11-16. Surveying attitudes and practices related to e-safety is one objective of the project. Others include to provide an insight into learners' use of Web 2.0 at home and school and to evaluate the impact on learning and teaching of Web 2.0 activities. The surveys involved more than 2,600 students and 206 teachers from a national sample of 15 schools and from 12 schools identified as systematically engaging in Web 2.0 activity. Surveys were also conducted with 76 parents from our participating schools and 45 parents from the Service, Management and Administrative listings of one of the research centres. In addition, focus groups have been held with students at 25 schools and interviews have been held with approximately 150 teachers, managers and technical staff. For the purposes of this paper we have combined data from both categories of school, except where indicated below, since the purpose here is to identify issues and form policy positions rather than to make comparisons or judgments.

Survey data

The survey data is from a questionnaire administered to 2611 children in Year 8 and Year 10 in two groups of schools: a national sample of 15 schools in England selected as representative of a range of school types and demographics, and a 'Web 2.0' sample of 11 schools that were identified by the researchers as supporting Web 2.0 activity across more than one discipline area. Not all questions were answered. The surveys were carried out in school classrooms, guided by researchers, and were preceded by a presentation to the class on Web 2.0.

The results showed that 64% of the respondents have wired internet access at home and 70% have wireless access. 74% of the respondents report having used social network (SN) sites, with 78% sharing files on SN sites occasionally or frequently.

Internet security

The respondents were asked direct questions to assess their use of instant message (IM) or email password. 9% indicated that they occasionally told their passwords to other people and 2% said they did so frequently (Table 1). It should be noted that the question did not differentiate between reporting a password to an adult, such as a parent, and to another child. 20% reported that they had occasionally learnt a password of another person, and 8% reported having done so frequently (Table 1). 23% reported that they never change their password, 37% do so rarely, 27% occasionally, and 9% frequently (Table 1).

	Doesn't apply to me	Never	Rarely	Occasionally	Frequently
"Have you told other people your password?"	7%	55%	26%	9%	2%
"I have become aware of other peoples' passwords."	5%	31%	35%	20%	8%
"I change the passwords I use."	3%	23%	37%	27%	9%

Table 1. Learner's email/IM password security

The survey also asked respondents to suggest a password of at least 6 characters "that you have not used before but which you think you could remember for accessing this survey". The choice of password (Table 2) provides an indication of their approach to internet safety. Half of the respondents provided a password based on personal information such as their date of birth or name of a family member that could be found from personal records. A further 25% used a password that could be found in a dictionary and so is vulnerable to a dictionary password-cracking program. This shows a worrying lack of security (though there is no evidence it is worse than the adult population) and there is a clear need to help children understand the risks of insecure passwords and how to prevent them.

Easy password	Password with a simple name or word	Password with personal information	Password including numeral(s)	Password including symbol(s)
5%	25%	52%	30%	5%

Table 2. Response to suggestion for a password.

Interactions with strangers

A series of items probed the young people's interactions with strangers. The survey offered response categories of 'never', 'rarely', 'occasionally' (approximately two times per month) and 'frequently' (approximately two times per week). Table 3 shows that 27% reported they had occasionally received an IM from a stranger, and 14% had received frequent such messages. Table 3 shows 20% having occasionally sent an IM

in reply to a stranger, and 15% having done so frequently. A similar pattern is shown for email messages (Table 3), though with lower rates of replying to strangers. 20% of the respondents indicated that they occasionally engaged in Instant Messaging or email correspondence with friends they had never met, and a further 17% indicated that they did so frequently (Table 3). Almost two thirds of the respondents had corresponded online with people they had not met face to face. The survey does not provide evidence as to whether these interactions are with adults or other children, nor whether or not they are inherently risky.

	Never	Rarely	Occasionally	Frequently
"On IM, I get messages from people I don't know."	23%	37%	27%	14%
"When I do, I would reply."	41%	25%	20%	15%
"On email, I get emails from people I don't know (not spam)."	31%	36%	21%	12%
"When I do, I would reply."	65%	20%	9%	5%
"I email/IM with online friends I have never met face-to-face."	35%	27%	21%	17%

Table 3. Emailing and instant messaging with people whom "I don't know"

As regards their use of social networking sites, 32% reported occasionally receiving friend requests from unknown people, with 22% receiving such requests frequently (Table 4). 29% occasionally accepted such requests, and 22% accepted them frequently (Table 4). 27% report occasionally maintaining online friendships with people they had not met in person, and 22% did so frequently (Table 4).

	Never	Rarely	Occasionally	Frequently
"I have friendship invitations from people I have never met."	19%	26%	32%	22%
"I have accepted such invitations."	29%	22%	29%	22%
"I keep up friendships with people I have never met."	29%	28%	27%	15%

Table 4. Social networking with "people I have never met"

The responses show that a substantial minority (42%) of children regularly interact socially online with people they have not met face to face. This does not, of itself, indicate that children are naïve or are engaging in behaviour that puts them at significant risk – that depends on the nature of the interactions. It does show that online interaction forms a different, though overlapping, social space to that of face to face friendships, involving friends of friends and people encountered in the online world, for example through multiplayer games. The survey did not ask whether the students had met offline with the people they had first encountered online.

Online bullying

In reply to questions about inappropriate social network activity, 13% of respondents who use these sites reported that people had occasionally posted pictures of them that they wished they wouldn't, with 3% reporting that this happened frequently (Table 5).

10% reported that people had occasionally written unacceptable things about them online, with 4% reporting such behaviour happening frequently (Table 5). Approximately half the respondents using these sites have been subject to unwelcome postings at some point. Such pictures or words may constitute overt bullying, or they may be unacceptable to the student for other reasons. Unwanted posting of text happened slightly more frequently at Web 2.0-innovating schools ($p < .05$) but incidents were reported to be rare in both Web 2.0 and normative sample schools.

	Never	Rarely	Occasionally	Frequently
"Others post pictures of me that I wish they wouldn't."	50%	32%	13%	3%
"Others write things about me that I wish they wouldn't."	54%	32%	10%	3%

Table 5. Unwanted postings of text and pictures

Interview and survey data with teachers

To provide a perspective from teachers, the project administered a questionnaire to teachers of all year groups in both the national sample schools and Web 2.0 schools. 130 teachers from the national sample responded, and 76 from the Web 2.0 sample. For the purposes of this report, we have not distinguished here between the categories of schools except where otherwise indicated. Interviews were also conducted with 67 teachers identified as classroom innovators with Web 2.0 technologies as well as 83 interviews with teachers from the national sample schools and 67 focus group interviews with pupils. These interviews necessarily offer anecdotal evidence, but they indicate tensions, issues and concerns not captured by the survey data.

The survey showed that around half of the teachers had engaged in Web 2.0 activities, almost exclusively for social use. Thus, 47% of teachers had created a personal profile on a social network website, with only 10% having done so for lesson planning or during school lessons. 30% had uploaded a video they had shot, with 12% doing so as part of school activity.

Only 55% of teachers surveyed indicated that their school had an eSafety policy, 3% believed that their school did not have such a policy, and 42% did not know. Teaching students about online safety was uncommon: 42% of teachers said they never did this, and only 11% did so frequently. Table 6 shows the reported prevalence of teachers' negative experiences caused by students using Web 2.0: 46% reported having had such a negative experience themselves, with 4% of teachers reporting that this occurred frequently.

	Never	Rarely	Occasionally	Frequently
"I have had negative experiences caused by students using Web 2.0."	54%	25%	18%	4%
"I have heard of another teacher having a negative experience caused by students using Web 2.0."	7%	30%	27%	35%

Table 6. Teachers' negative experiences caused by students using Web 2.0

Online bullying

The main concern expressed by teachers is about how much information children actually or might give away about themselves. This was a mixture of anxiety about online bullying and strangers contacting identified pupils. The teacher survey data indicated that 42% of teachers agree that online bullying is currently a problem, with a further 13% strongly agreeing (Table 7).

Strongly agree	Agree	Disagree	Strongly Disagree
13%	42%	14%	2%

Table 7. Teacher response to “Bullying through online postings is currently a problem”

One teacher described an incident where some girls had posted quite provocative photos of themselves on Bebo, assuming that only other children of their age were accessing the site. In another incident, a student sent a suggestive video to a boyfriend who then distributed it to other pupils and the video spread through the school. The school responded by confiscating mobile phones to delete the video and excluding the offender, discussing this with the pupils. Students were very aware of this incident.

A consequence of online activity is that bullies generally leave a record of their actions that can be traced to its originator. One school had problems with children posting playground and classroom activities to YouTube, but reported that the offending pupils generally admit responsibility when faced with the evidence and are co-operative about removing and destroying inappropriate material.

Schools are beginning to extend their bullying policies to include the internet:

“A couple of instances of online bullying but this is seen by senior management as a bullying issue and not an IT issue.” (ICT Coordinator from Web 2.0 school)

“We’ve had instances as every school of things being posted onto YouTube that we’ve had to tackle. ... If in the past bullying has been a word in a playground or a name written in a book. Well all it is now is a posting on a website. You don’t have to be scared about. All you have to do is to say here is a piece of evidence, you did it, we’ll now proceed just as we would in any other case. The thing with Web 2.0 is that it is not removable. And it sits there. I think that will be the issue that society needs to think through.” (Deputy Head Teacher from Web 2.0 school)

The quotation highlights a difficulty of removing material from social network sites, particularly if it has been copied and stored on children’s computers and media players. Schools will need to address this issue whether or not they adopt Web 2.0 technologies, since one possible route to online bullying is for a child to use a personal phone to capture an image and a home computer to post a hurtful message.

Personal information

In relation to strangers reading information posted by children, the underlying tension was typically expressed by teachers in terms of a 'worst case' incident and the effect that might have on the school's reputation.

"If it's going to be related to the school, I think that you have to make sure that everything is moderated. Not that I'm saying that the pupils would say inappropriate things, but if they were to do that then obviously that would reflect badly on the school, therefore I would feel uncomfortable about letting the kids do that unless everything was moderated." (Teacher from Web 2.0 school)

Some interviewees indicated that schools were prevented by media scare stories from providing the kind of Web 2.0 activities that are now part of society:

"The argument is internet safety. Child grooming, which is absolutely ridiculous. I'm of the belief, you know, statistics and everything show that a child is more likely to come to harm inside the four walls of their house by a relative than they are by a total and complete stranger." (Teacher from Web 2.0 school)

"I am very much limited by my institution and their rules and policies and ... you go onto some other websites and God knows what the kids access at home." (Teacher from Web 2.0 school)

A frequently-occurring tension is the blocking of internet sites causing difficulties for legitimate schoolwork. In some cases, the blocking is done by outside agencies, particularly Local Authorities.

"We can't always reliably hope to pursue a route because we don't know if a technology will be made available to us. And sometimes it's beyond the school's control." (ICT/Art teacher).

"Everything is blocked basically...[by the Local Authority] and that to me defeats the object of the internet" (ICT Coordinator).

"When teachers ask you to get like multimedia files for Powerpoints and stuff you like say to them, 'I can't get them because you've blocked the sites on the internet' so they say, 'oh you can do it at home,' but that's really not fair." (Year 10 student).

One teacher reported that the school had ICT resources for children, but had not yet found "their voice".

In some schools, there appears to be a culture of collusion by teachers and pupils to overcome school restrictions and satisfy their perceived needs, such as carrying out collaborative project work. In a few schools, password sharing is reported as a frequent activity.

“Out of a class of 24, every single person knew somebody else’s password and username to get onto the system.” (ICT teacher).

“A lot of kids do have a slight understanding about dangers but they just put it at the back of their mind.” (Head of ICT).

Tensions

Tensions arise from the responsibility of schools and Local Authorities to provide a safe online environment, resulting in a school Virtual Learning Environment (VLE) being cut off from the resources and interactions of the public internet. One view is that to move outside the protection of a closed and moderated space is to expose children, teachers and the school to unnecessary risk; another is that providing a protected area fails to teach children essential skills of managing their online identity and encourages them to subvert the restrictions. There is general agreement that children are finding ways to bypass internet filters through the use of proxy sites. For example, pupils in a girls’ school were familiar with the use of proxy bypass sites. They have email and social network sites open for general chat during lessons, but minimise the window when a teacher moves near.

Some schools are struggling to establish guidelines for appropriate behaviour in this new sphere of social interaction. One interview referred to the ‘minefield’ around teachers communicating with pupils out of school hours. It also identified plagiarism (by copying text from websites) and cyber-bullying as significant problems. Another interview, by contrast, indicated that the school had set guidelines for responsible behaviour and that its pupils generally behaved appropriately within them.

Schools had varying arrangements for dealing with filtering, blocking and monitoring: some performed these functions in-house, others externally. Schools varied in the degree to which their access to sites depended on the guidelines set by the LA. In a small number of schools there was a lack of communication or understanding about how to un-block a desired site. According to teacher interviews, the time needed to un-block a site varied from a few minutes to a few weeks.

An over-arching issue is a failure of partnership and attribution of blame to others. Thus, the children interviewed in focus groups generally indicated that they were well aware of internet dangers but were not trusted to self-regulate their behaviour. Some teachers stated that children were naïve in not safeguarding their passwords and in giving out personal information online. Some also regarded parents as being out of touch with new developments and incapable of imposing appropriate safeguards. A few teachers criticised the Local Authority for over-zealous imposition of internet filters, prohibiting the schools from using the internet for legitimate schoolwork.

Cooperative approaches

An indication of a cooperative approach to internet safety comes from a school where a few students had persistently broken through internet filters. These students have been supervised by the ICT Assistant Head who has them trialling new software, researching career paths, and presenting to governors. The subversion still happens but is “not malicious” (ICT Assistant Head).

A teacher in a Web 2.0 active school described how the school is working to establish a policy for managed use of the open Web.

“Teachers can request websites to be opened up, but it’s very cumbersome and it’s not used particularly well, so over the last three, four years we’ve got a fair number of websites that have been opened up, but they’re all very much for educational use. So last month I worked with the school council to put together a proposal to management that we would have, I think what we’re going to go with as of next week is open access to the web for pupils and that would be two half-hour slots in the week. And there’s obviously a contract that they’ve got to sign before we hand, and they realise that not everybody can just come and descend on one room to get access, so it’s going to be very, very managed.” (Teacher in Web 2.0 school)

The survey and focus group interviews have indicated substantial tensions and issues for schools in forming policy on Web 2.0 activities. Schools need to take account of unease from parents about their children conversing with strangers and the fear, however unlikely, of them falling prey to internet predators. They must manage online bullying and the posting by children of inappropriate material on websites. They need to help children develop appropriate etiquette and to know when social networking becomes risky and unacceptable. Most of all, schools, supported by agencies including Becta, need to develop an approach to the social internet that complements home use while developing a distinctive educational space for creativity, community and personal learning.

Survey data with parents

Our survey of 121 parents indicated that most feel they have a better understanding of technology than their children: only 13% report that they know less about computers and technology than their children do. Table 8 illustrates how some of these concerns are represented amongst the sample of parents we surveyed. Although only 17% of parents agree or strongly agree that they worry about their child being at risk of online bullying, concern is greater regarding contact from inappropriate adults (23% strongly agree, 44% agree); accidental exposure to inappropriate material (15% strongly agree, 59% agree); and children’s visits to unapproved web sites (13% strongly agree, 55% agree).

	Strongly agree	Agree	Disagree	Strongly Disagree
“I am concerned about inappropriate adults contacting my child online.”	23%	44%	28%	5%
“I worry that my child might accidentally see inappropriate material on the internet.”	15%	59%	23%	2%
“I worry that my child might visit web sites I wouldn’t approve of.”	13%	55%	32%	1%
“I worry that my child is at risk of being bullied online.”	2%	15%	66%	17%

Table 8. Parents’ opinions about risks involved in children’s use of technology

Despite widespread concern about exposure to inappropriate content and individuals on the internet, most parents remain positive about using technology to support their children’s education. 91% of parents surveyed agree or strongly agree that every child should have strong technology skills and 94% believe that the internet may be useful in subjects other than ICT. Most parents also view the internet as a good way for their children to keep in touch with school friends (8% strongly agree, 54% agree).

Like the schools in our sample, most of the parents surveyed (66%) indicated that they had measures in place to prevent their children from visiting websites of which they disapprove. Some parents volunteered that these measures included, saving instant messenger conversations without a child’s knowledge, password-protecting certain websites, locating the computer in a shared area of the home, and discussing e-Safety with their child. Parents generally trust their children to conduct themselves safely online, with 66% agreeing or strongly agreeing that their child knows how to create secure passwords and 62% agreeing or strongly agreeing that their child would not disclose personal details on the internet (see Table 9).

	Strongly Agree	Agree	Disagree	Strongly Disagree
I have measures in place to prevent my child visiting websites I disapprove of	24%	42%	27%	8%
I believe that my child knows how to create secure passwords	22%	44%	28%	4%
I think my child would never disclose personal details on the internet	15%	47%	33%	4%

Table 9. Parents’ opinions about children’s online safety behaviour

Policy Delphi workshop

The survey and focus group interviews were intended to gather intelligence, not to explore positions or to seek resolutions and policy options. For this purpose, the project formed an e-safety and Web 2.0 Advisory Panel comprising thirty people in the UK with specific expertise in e-safety and in enabling creative use of web technology. The range of organisations and perspectives they represent include internet safety organisations, alternatives to traditional schooling, Local Authorities, government policy makers, and educational software companies. They were invited to a Policy Delphi Workshop at the University of Nottingham, which 23 attended. The aim of the Delphi workshop was to review initial findings from the surveys and interviews, to articulate positions relating to e-safety and Web 2.0 activity, and to explore the implications of these positions for education and policy. The Policy Delphi method (Linstone & Turoff, 1976) is a structured group process to survey and collect the opinions of experts on a complex problem. Rather than striving for an early consensus, the emphasis is on identifying differing positions through a process of structured debate. A ‘position’ for this purpose is an informed viewpoint, which should be defensible, but not necessarily held by all, or any, of the participants.

One method to assist the generation of positions is to look for ‘dimensions of difference’, axes along which opinions differ. Through paired and then plenary

discussions the workshop produced a set of dimensions. For example, one dimension was “Responsibility” with a range from “Individual” to “Community” (Figure 1).

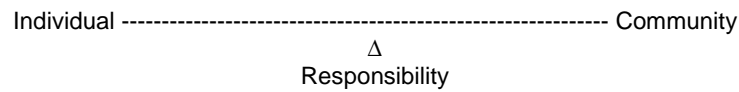


Figure 1. A ‘dimension of difference’ from the Policy Delphi Workshop

Pairs of dimensions can be combined so that they form orthogonal axes. Each quadrant of the resulting diagram indicates a possible policy position. Two axes identified at the workshop resulted in a set of positions that especially matched the concerns and issues identified from the surveys and interviews. These were ‘Support’ and ‘Access’, which produced a set of positions shown in Figure 2.

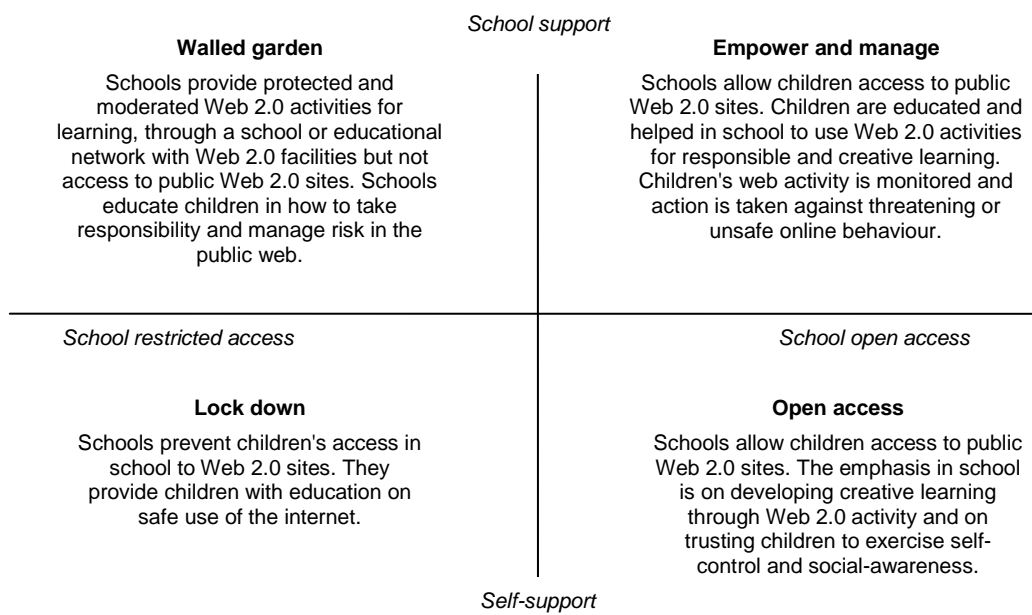


Figure 2. Policy positions produced from the ‘dimensions of difference’.

The Support dimension ranged from self-regulation, to school support for educating children in responsible internet use and monitoring of their activities. The access dimension ranged from prohibiting all access in school to Web 2.0 activities, to open access to Web 2.0 sites. For ease of reference, the positions in the four quadrants were labelled and the workshop produced short descriptions of the implications of each position for education and for policy.

A significant problem with the approach taken by the Policy Delphi Workshop is that it can lead to polarised positions. Each ‘dimension of difference’ is a scale rather than a dichotomy. However, a first step is to treat the differences as significant, since they have resulted in a set of defensible positions that can be identified with sincerely, sometimes passionately, held ethical viewpoints. The ‘Open access’ position represents a libertarian perspective of educating children to personal freedom and responsibility. The ‘Lock down’ position is indicative of social control. ‘Empower and manage’ is the ‘freedom within the law’ typical of a participatory democracy.

And ‘Walled-Garden’ is the Enlightenment philosophy of creating a rich and safe environment in which to nurture young minds. The UK education system has sought to find a stance within these competing viewpoints from which to form a consensual school ethos and curriculum. The challenge is to continue this process with new technologies, opportunities and risks.

In the second part of the Delphi process, the Advisory Panel were asked to critique the positions on a web discussion list. For the final stage, all members of the Panel, plus members of the research team, ranked the four positions, first for desirability (“How desirable is it that the UK schools should adopt the position?”) and then for feasibility (“How feasible do you think it will be for UK schools to adopt the position over the next three years?”). In making the rankings, the Panel were asked to consider the following:

- The context is Web 2.0 technologies for learning by children aged 11 – 16 in UK schools.
- There should be a balance between enabling children to develop the creative skills and knowledge for learning in the 21st century, and providing a safe and non-threatening environment for education.

This exercise produced a general consensus on the most desirable position (with some dissention) but not on which would be most feasible. Table 10 shows, for each position, the number of respondents indicating each rank.

	Desirability				Feasibility			
	First	Second	Third	Fourth	First	Second	Third	Fourth
Empower and Manage	13	5	0	0	6	4	7	1
Lock Down	0	0	1	16	6	2	3	7
Open Access	4	6	6	1	1	2	5	7
Walled Garden	1	7	10	0	4	9	2	1

Table 10. Results of the ranking exercise for four policy positions on Web 2.0 and e-safety from the Expert Advisory Panel.

The comments of the panellists indicate their agreement that children should be empowered and supported by schools to engage in safe and creative use of the public Web, with their activities being monitored and moderated. All the quotations below are from comments provided as part of the ranking exercise.

“Although this requires more work than giving open access, schools are already showing monitoring is possible and successful.”

Some respondents indicated that, whereas they may be attracted to the principle of open access, the duty of care by schools means that it is not appropriate at this stage. Even those advocated open access indicated the need for moderation.

“[Open access] would be the most desirable but sadly there will always be some individuals who do not behave responsibly (putting themselves and others at risk).”

“I was torn about whether to put Open Access or Empower and Manage first for desirability. ... Moderation is a key element in how you ‘educate and empower’ – it also helps keep the discussions focused! ... When I say moderation I also mean ‘post-moderation’ rather than ‘pre-moderation’ – so kids should be free to post and moderation should be applied after their posts have gone live. It is also important (and part of how students are educated) that they are involved in and (partially) responsible for the moderation.”

One respondent (a member of the project team) offered an argument for a ‘big walled garden’ approach, with a set of managed educational services for schools, set apart from the public web.

“I’ve totally changed my position on walled gardens since interviewing RBC [Regional Broadband Consortium] and LA [Local Authority] leaders – some of the larger walled gardens are now going to have 1.5 million accredited users and the capability of setting up additional local, national and international shared areas with other users. I share the view of those RBC managers who say ‘there are no barriers to Web 2.0 use – we’ve eliminated them.’ When the garden’s this big, the walls are not a barrier to educationally worthwhile internet use.”

Others indicated that although this position may satisfy the public, it could create an illusion of safety and require continual IT support.

“The web is constantly changing. This would require the IT teams to be constantly making tools available within the garden which would not necessarily be possible as they may need to host a specific technology. Walled garden also stops students from exploring sites and developing their own personal ideas of what is appropriate or is actually usable.”

There was no support from the Advisory Panel for the ‘Lock down’ position of excluding children from Web 2.0 activities at school, even though this is the situation at most schools in the UK.

“This would be a disaster, in my view.”

“In my view this is unacceptable from an educational perspective, however I believe that this will be a very attractive position for some areas of society, particularly in the light of sensationalist media coverage around cases involving grooming and internet abuse.”

The contrast between what is desirable for education and society and what is currently feasible was succinctly captured by one respondent:

“It is interesting that I consider desirability and feasibility to be opposites ... never thought of that before ... Feasibility is about fear/time/money/will/politics. Desirability is about excitement/vision/risk/androgogy.”

Conclusions

At present, schools are caught between the rock of parental fears about internet abuse and the hard place of helping children to develop responsible and creative use of Web 2.0 for learning. On their own, schools will find it difficult to develop a policy for appropriate use of Web 2.0 to support children’s learning and skills development. Most are likely to continue to prevent access to social network sites, claiming a duty of care in response to the worst case risks.

Schools do not forbid children from walking unaccompanied to school because of the risk of a child being abducted, or injured crossing a road. They do not prevent general access to the school playground because of incidents of bullying. In these areas, policy has evolved over time to balance the likely risks against the benefits to children of exercise and creative play, also taking account of pragmatic issues such as difficulty of prevention and the value of getting children out of the school buildings over break time. For younger children, schools provide supervision at play and training in road safety, as well as instilling school rules of acceptable behaviour.

The reasons why such an approach has not evolved for internet safety is evident from the interviews with teachers. The Web is a new medium, in the spotlight of the press. Despite a desire from some teachers to explore its benefits for creativity and social learning, they are constrained by restrictions set by Local Authorities and school governors. Most Web 2.0 schools we surveyed are providing constrained opportunities for social networking through additions to their school VLE, but a few are providing managed access to some public social network websites, after negotiation to remove restrictions. Any substantial change cannot come from teachers alone; innovating teachers and schools need the support of policy makers and Local Authorities. The evidence from this study is that children are engaging with a wide range of social, creative and engaging web activities at home and this is producing a growing divide between such web-confident children and those who are restricted to using the web at school to retrieve specific information from pre-approved websites.

To overcome the new digital divide between the web-confident and web-restricted children will require combined effort by policy makers, Local Authorities, teachers, parents and students and this can only happen in a series of stages. A necessary pre-requisite is to balance discussion of e-safety and child protection with that of web entitlement and child development.

In relation to Web 2.0 implementation in schools, the expert panel showed a clear preference at Key Stages 3 and 4 for a process of empowerment and managed access to the public web. This would involve building on current good practice from those schools that are venturing into Web 2.0 territory. School governors will need a balanced assessment of the benefits and risks. Schools will need assistance to develop a policy of managed access, with appropriate tools for monitoring web use, and an

ethics policy to establish the rights and responsibilities of staff and students. Policy on bullying will need to be extended, if it is not already, to cover internet bullying and harassment. Teachers will need support in developing new teaching practices that embrace creative and social learning on the web and in promoting responsible internet use. Issues of posting personal details on social networked sites will need to be debated. Parents will need to be continually reassured that the web can be a valuable place for learning and that schools have effective policies and practices for safe use.

Although the panel members, with one exception, did not support the development of a 'walled garden' of educational Web 2.0 services for older students, this approach may be more appropriate for younger children. Children's social network sites such as Habbo Hotel are already successful and similar tools could be developed, such as online picture albums, scrapbooks, and video diaries, hosted on age-restricted sites. These might be accompanied by 'web proficiency' tests, similar to cycling proficiency ones where children can be taught the rules of web safety and can demonstrate responsible use..

This will be a gradual process of building trust and experience and of understanding and guiding children's development of skills in social interaction and creativity on the web. There will be inevitable setbacks as the press and television highlight cases of internet bullying and schools allowing pupils to socialise online. Over time, the social web will become absorbed into education, just as other media have before it. It is fitting to end with a quotation from another era, expressing similar concerns about the dangers to children from new media:

"To try to safeguard children without knowing what really endangers them, to set out to please them without knowing their tastes or understanding their development is to court failure ... negative criticism must be accompanied by constructive efforts." (Bauchard, 1953, p. 14)

Acknowledgments

The research described in this paper was commissioned by Becta as part of the project 'Web 2.0 Technologies for Learning at Key Stages 3 and 4' carried out by Nottingham University in conjunction with London Knowledge Lab and Manchester Metropolitan University. Reports from the project are available on the Becta website: http://partners.becta.org.uk/index.php?section=rh&catcode=_re_rp_02&rid=14543. The paper draws on work carried out by the project team, comprising Charles Crook, John Cummings, Tony Fisher, Rebecca Graber, Colin Harrison, Cathy Lewin, Kit Logan, Rose Luckin, Martin Oliver and Mike Sharples. We wish to thank the schools, children, teachers and parents who participated in the surveys and interviews..

References

Bauchard, P. (1953) *A Report on Press, Film and Radio for Children*. Paris: UNESCO.

- Byron, T. (2007) *Safer Children in a Digital World: The Report of the Byron Review*. London: Department for Children, Schools and Department for Culture, Media and Sport. Retrieved 16/07/2008 from <http://www.dfes.gov.uk/byronreview/>.
- Cassell, J. & Cramer, M. (2007) Hi Tech or High Risk? Moral Panics about Girls Online. In *Digital Youth, Innovation, and the Unexpected: The MacArthur Foundation Series on Digital Media and Learning* (ed. T. MacPherson), 53-75. Cambridge, MA: MIT Press.
- Green, H. & Hannon, C. (2007) *TheirSpace: Education for a digital generation*. London: Demos. Retrieved 16/07/2008 from <http://www.demos.co.uk/publications/theirspace>.
- Li, Q. (2006) Cyberbullying in Schools: A Research of Gender Differences. *School Psychology International*, 27 (2), 157-170.
- Linstone, H. A. & Turoff, M. (1976) The Delphi Method: Techniques and Applications. *Technometrics*, 18 (3), 363-364.
- Ofcom (2007) *Children and the Internet: Consumer Panel Report*. London: Ofcom.
- O'Reilly, T. (2005) What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. Retrieved 16/07/2008 from <http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html>.
- United Nations (1990) *Convention on the Rights of the Child*. United Nations Office of the High Commissioner for Human Rights. Retrieved 16/07/2008 from <http://www.unhchr.ch/html/menu3/b/k2crc.htm>.
- Wolak, J., Finkelhor, D., Mitchell, K.J., & Ybarra, M.L. (2008) Online "Predators" and Their Victims: Myths, Realities and Implications for Prevention and Treatment. *American Psychologist*, 63 (2), 111-128.
- Wright, E. R. and Lawson, A. H. (2004,). *Computer-Mediated Communication and Student Learning In Large Introductory Sociology Courses*. Paper presented at the annual meeting of the American Sociological Association, Hilton San Francisco & Renaissance Parc 55 Hotel, San Francisco, CA. Retrieved 16/07/2008 from http://www.allacademic.com/meta/p108968_index.html.