E-safety and Web 2.0

Web 2.0 technologies for learning at Key Stages 3 and 4

Mike Sharples, Rebecca Graber, Colin Harrison and Kit Logan

On behalf of the full project team:
Dr. Charles Crook, LSRI & School of Education, University of Nottingham
John Cummings, Manchester Metropolitan University
Tony Fisher, School of Education, University of Nottingham
Rebecca Graber, University of Nottingham
Prof. Colin Harrison, School of Education, University of Nottingham
Dr. Cathy Lewin, Education and Social Research Institute, Manchester Metropolitan University
Dr. Kit Logan, London Knowledge Lab, Institute of Education
Prof. Rose Luckin, London Knowledge Lab, Institute of Education
Dr. Martin Oliver, London Knowledge Lab, Institute of Education
Prof. Mike Sharples, LSRI & School of Education, University of Nottingham

© Becta 2008

Contents

Executive summary **4**
Locating this report within the Web 2.0 project **8**
Background **9**
Society's fears **10**
Benefits of Web 2.0 activity 11
Risks of Web 2.0 activity 13
Inappropriate content 13
Abuse of children 13
Online bullying 15
Cheating online 16
Findings from the Becta Web 2.0 project related to e-safety **17**
Survey data 17
Internet security 17
Interactions with strangers 18
Online bullying 20
Interview and survey data with teachers 20
Online bullying 21
Personal information 22
Tensions 23
Co-operative approaches 24
Survey data with parents 25
Policy Delphi workshop 27
Conclusions **33**
Resources **36**

© Becta 2008

List of tables and figures

Table 1: Learner's email/IM password security 18
Table 2: Response to suggestion for a password 18
Table 3: Emailing and instant messaging with people whom 'I don't know'..... 19
Table 4: Social networking with 'people I have never met' 19
Table 5: Unwanted postings of text and pictures..... 20
Table 6: Teachers' negative experiences caused by students using Web 2.0 21
Table 7: Teacher response to 'bullying through online postings is currently a problem' 21
Table 8: Parents' opinions about risks involved in children's use of technology..... 26
Table 9: Parents' opinions about children's online safety behaviour 27
Figure 1: A 'dimension of difference' from the Policy Delphi workshop 28
Figure 2: Policy positions produced from the 'dimensions of difference' 29
Table 10: Results of the ranking exercise for four policy positions on Web 2.0 and e-safety from the advisory panel 30

© Becta 2008

Becta has commissioned the University of Nottingham in conjunction with London Knowledge Lab and Manchester Metropolitan University to research Web 2.0 technologies for learning at Key Stages 3 and 4.This is the fourth report from that research and concentrates on the e-safety aspects of Web 2.0 in education.

For more information, and to access other reports from the project, see: http://partners.becta.org.uk/index.php?section=rh&catcode=_re_rp_02&rid=14543

Executive summary

The central challenge for schools in considering the adoption of Web 2.0 technologies is how to support children to engage in productive and creative social learning while protecting them from undue risks.

Companion reports from the Web 2.0 project have indicated benefits to young people from engaging in online social networking. They can create portfolios of digital media, engage in peer teaching, and develop their confidence and voice. Evidence gathered from the Web 2.0 project indicates 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 for content retrieval.

The reasons why most schools are not encouraging the use of Web 2.0 for learning are apparent from our interviews with teachers and pupils. The World Wide 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 real or perceived limitations set by local authorities and school governors. In an increasingly risk-averse society, where schools and local authorities are vulnerable to legal action by parents, there is a strong incentive to avoid the ‘worst-case’ risk to children from internet predators and abusers.

If schools are to develop effective policy for adopting Web 2.0 technologies, it is important to distinguish the current fears of society from evidence of actual risk to children. These fears relate to children being exposed to inappropriate content, children being lured into exhibiting inappropriate behaviour, children being abused by strangers and online bullying.

The abuse of children through the internet is a direct consequence of the facilities afforded by the social internet. The evidence so far is that the risk of children being duped by online predators is small and the public image of online predators who trick naive children into becoming victims of abuse is largely inaccurate. In most cases, the victims are aware they are conversing online with adults and offenders rarely

© Becta 2008

deceive victims about their sexual interests. Most victims who meet offenders face to face go to such meetings expecting to engage in sexual activity.

An important concern is that posting personal information on social websites such as Facebook, MySpace and Bebo is putting children at risk of abuse. Our survey of children at Key Stages 3 and 4 shows 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 naive or engaging in behaviour that puts them at significant risk. Rather, it shows 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.

Schools can have a role in educating children to use the new internet safely and responsibly. Teachers can help children to appreciate when they cross the line from normal and acceptable Web 2.0 activity, which may include posting some personal details online, to abnormal and risky behaviour. Currently, most children are prevented from engaging in any social activity on the web at school. 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 for society at large. Now that most children have home access, safe behaviours are essential, but a strongly protected online environment at school may not provide the opportunity to learn these.

Online bullying, or 'cyberbullying', can be an upsetting experience and a recent phenomenon is the posting of hurtful images and videos on the web. Social networking and media-sharing websites enable children to write abusive messages on discussion boards and contribute to sites that criticise their teachers and schools. The survey responses suggest that cyberbullying is seen as a frequent or occasional problem by some 15% of children and that approximately half have been subject to unwelcome postings at some point. Schools are beginning to extend their bullying policies to include the internet. They will need to address this issue whether or not they adopt Web 2.0 technologies, since the most likely route to online bullying is for a child to use a personal mobile phone to capture an image and a home computer to post a hurtful message.

A further concern of schools, not given prominence in the press, 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. They can communicate by text messages within the classroom and, increasingly, they are able to access the web through a mobile phone.

Our interviews with teachers showed that around half of them had engaged in Web 2.0 activities, almost exclusively for social use. The main concern expressed by

© Becta 2008

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. 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 child and on the school community. Some interviewees said that schools were prevented by media scare stories from providing the kind of Web 2.0 activities that are now part of society.

A tension identified by the teachers is the blocking of internet sites, causing difficulties for legitimate schoolwork such as online research, media creation and collaborative project work. There is general agreement that children are finding ways to bypass internet filters through the use of proxy sites. 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.

An overarching issue is a failure of partnership and attribution of blame to others. Thus, the children interviewed generally answered that they were well aware of internet dangers but were not trusted to self-regulate their behaviour. Some teachers stated that children were naive 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.

To seek expert opinion, the project formed an e-safety and Web 2.0 advisory panel comprising 30 people in the UK with specific expertise in e-safety and in enabling creative use of web technology. In a workshop session, 23 members of the panel proposed and discussed a set of policy positions on school adoption of Web 2.0 technologies at Key Stages 3 and 4. In an email survey, the same panel were asked to rate four of the positions for desirability and feasibility. These positions, further explored in the report, were:

- **Walled garden** – Schools provide protected and moderated Web 2.0 activities for learning, through a school or educational network with Web 2.0 facilities but not access to public Web 2.0 sites. Schools educate children in how to take responsibility and manage risk on the public web.
- **Empower and manage** – Schools allow children access to public Web 2.0 sites. Children are educated and helped in school to use Web 2.0 activities for responsible and creative learning. Children's web activity is monitored and action is taken against threatening or unsafe online behaviour.

© Becta 2008

- **Lock down** – Schools prevent children's access in school to Web 2.0 sites. They provide children with education on safe use of the internet.
- **Open access** – Schools allow children access to public Web 2.0 sites. The emphasis in school is on developing creative learning through Web 2.0 activity and on trusting children to exercise self-control and social awareness.

This exercise produced a general consensus on 'empower and manage' as the most desirable position for Key Stages 3 and 4, but not on which would be the most feasible to implement. The comments of the panellists indicated 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.

The survey and focus group interviews have highlighted 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. Policy-makers need to balance discussion of e-safety and child protection with that of web entitlement and child development. 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.

© Becta 2008

Locating this report within the Web 2.0 project

The Becta research project on Web 2.0 technologies for learning at Key Stages 3 and 4 has five primary objectives:

1. To present an overview of current research into Web 2.0 and its potential uses in education.
2. To provide insight into learners' use of Web 2.0 both at home and at school.
3. To evaluate the impact on learning and teaching of Web 2.0 and opportunities presented by its use in education.
4. To investigate barriers and challenges to implementation by evaluating experiences across local authorities.
5. To identify e-safety and child protection issues surrounding the use of Web 2.0 and identify how these technologies can be used safely.

The present report is focused on the last of these objectives. It begins by examining existing research for an understanding of the current landscape in which e-safety and Web 2.0 issues play out, and current opinions by experts on how best to navigate the challenges of supporting safe use of Web 2.0 tools. The report then draws upon a significant data set to make its own original contributions of understanding and evaluation. The research team conducted in-depth investigations of 27 schools across the country. Online surveys and focus groups were conducted with more than 2,600 learners at Key Stages 3 and 4, 100 interviews and 206 online surveys were conducted with teachers, and online surveys of a cross-section of parents were also carried out. A Policy Delphi conference brought together leading experts to evaluate the feasibility and desirability of possible strategies for utilising Web 2.0 in education. The data from the project therefore presents a significant opportunity to gain detailed understanding of the significant e-safety and child protection issues raised by Web 2.0 from a variety of informant and expert perspectives.

This report builds upon the framework established in the project's first report, *The Current Landscape – Opportunities, Challenges and Tensions* (see objective one in the list above). Other reports have provided detailed analysis of learners' use of Web 2.0 both at home and at school (objective two), and have evaluated the opportunities and impact of Web 2.0 on learning and teaching, as well as barriers and challenges to implementation (objectives three and four).

© Becta 2008

Background

The 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 the web 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. The central question that schools must address in a consideration of e-safety and Web 2.0 activity is: How can they support children to engage in productive and creative social learning through web technologies while protecting them from undue risk?

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.[1] 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 dilemma 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 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.

[1] http://www.unhchr.ch/html/menu3/b/k2crc.htm – accessed September 2008.

Society's fears

For over half a century, adults have sought to protect children from the perceived dangers of new media. In the middle of the 20th century, the concerns were about risks to children from comic books, films and radio. A substantial report published by UNESCO in 1953[2] discussed the effects of press, film and radio on children:

> "The radio as a medium of information is all-pervading; it may also be harmful. Anything heard on the radio is taken as gospel truth. Songs are picked up at once and sung by everyone. Various attempts have therefore been made by teachers and educationalists to introduce new children's songs and to raise the standards of children's broadcasts through the use of new methods."[3]

> "In the few countries where an effort has been made to produce films specially intended for children and to organise cinema clubs and performances for children, their results appear to have been most encouraging. This does not alter the fact that enterprises such as these at present affect only a very small percentage of children, and that even the children who attend the special performances continue to see a large number of films for adults."[4]

Needless to say, despite efforts to broadcast children's radio and run cinema clubs, children have continued to sing popular songs from the radio and watch films intended for adults. As for the medium of television, which was just entering homes in 1953, the report stated "that problems will arise there can be no doubt" since, the author argued, television shared 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 cited evidence that children in some parts of the United States were spending nearly four hours a day 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, entitled *Safer Children in a Digital World*.[5] Both warn against the encroachment of a new medium (in the latter's case, the internet) into children's lives; they criticise sensational accounts of the dangers but are concerned about

---

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

[3] Ibid, p93.

[4] Ibid, p91.

[5] Byron, T (2007), *Safer Children in a Digital World: The Report of the Byron Review,* London: Department for Children, Schools and Families [http://www.dcsf.gov.uk/byronreview].

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 well-being.

It would appear that a new mass medium becomes an emblem for society's unease about modernity. As children so readily adopt the medium and make it their own, showing an ease with the technology and developing a culture that excludes adults, it 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 (for example, claims that children are spending 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 report suggests that "many of the issues that have traditionally been discussed around media influence on children are relevant to the internet, such as violence and its effect on behaviour and attitudes".[6] It then suggests that there are new risks to children from the internet, including: ease of access for users; abundance of material available; ubiquity and affordability; the interactivity of the medium; the potential for users to share material; the degree of anonymity that users can enjoy; and the lack of 'gate-keepers' or authorities that might restrict access. The report concludes that families, industry, government and others in the public and third sectors should all play their part "to reduce the availability of potentially harmful material, restrict access to it by children, and increase children's resilience".[7]

The Byron Review has already been influential in raising considerations of e-safety among 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, it was only asked to make an assessment of risk, not benefit.[8]

Benefits of Web 2.0 activity

Safe internet use requires balancing perceived benefits against acceptable risks. Companion reports from the Web 2.0 project 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,

[6] Ibid, section 3.24, p48.

[7] Ibid, executive summary, p2.

[8] "Carry out an independent review of the risks children face from the internet and video games." Ibid, foreword, p1.

© Becta 2008

presentation, leadership, team-building, confidence, communication, innovation, initiative, critical awareness in information gathering, and ability to evaluate, question and prioritise information.[9] 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[10] 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:

> "To be an effective World of Warcraft guild master, one needs to be adept at many skills: attracting, evaluating and recruiting new members; creating apprenticeship programmes; orchestrating group strategy; and managing disputes. All of these skills are readily welcomed in the modern workplace, and they are set to become even more valuable."[11]

As Green and Hannon point out, 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."[12]

To promote Web 2.0 as a new learning space risks turning it into an extension of formal schoolwork. This is starting to happen as some schools use wikis to promote creative writing, podcasts to deliver curriculum materials, and blogs as reflective diaries. Such activities may well be educationally valuable and make good use of technology for classroom learning, but they are not Web 2.0 activities in the wider sense of the term, that is, to embrace personal ownership and sharing of data and an architecture of participation and social networking.[13] Computer-supported collaborative and social learning is being explored by a few schools in the UK and worldwide, but for this to be adopted more widely requires the development of new

---

[9] Green, H and Hannon, C (2007), *Their Space: Education for a Digital Generation*, London: Demos and Grunwald Associates, L (2007), *Creating and Connecting/Research and Guidelines on Social and Educational Networking*, National School Boards Association. Cited in *Final Report for Becta, KS3 and KS4 Learners' Use of Web 2.0 Technologies In and Out of School*.

[10] Green, H and Hannon, C (2007), *Their Space: Education for a Digital Generation,* London: Demos [http://www.demos.co.uk/publications/theirspace – accessed 22 May 2008].

[11] Ibid, p23.

[12] Ibid*,* p23.

[13] http://en.wikipedia.org/wiki/Web_2 – accessed 22 May 2008.

© Becta 2008

methods of teaching and assessment for Key Stages 3 and 4 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. These fears relate to children being exposed to inappropriate content, children being abused by strangers, and online bullying.[14]What is the evidence that these pose real risks to children at Key Stages 3 and 4?

Inappropriate content

Inappropriate content ranges from advertising (for fattening foods and sweet drinks, for example) 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 to see at different stages of their development.

Abuse of children

By contrast, the abuse of children by adults through the internet is a direct consequence of the facilities afforded 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".[15] It cites an Ofcom report[16] in saying that: "Adults masquerading as younger people is one of the biggest issues parents say they are most concerned about with the internet."[17] 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[18] of internet abuse cases in the United States, published in *American Psychologist*, concludes that "the publicity about online 'predators' who prey on naive children using trickery and violence is largely inaccurate".[19] The report states that the reality

[14] Byron Report, p4.

[15] Ibid, paragraph 3.50, p53.

[16] Ofcom (2007), *Children and the Internet: Consumer Panel Report,* London: Ofcom.

[17] Byron Report, paragraph 3.50, p53.

[18] Wolak, J, Finkelhor, D, Mitchell, K J and Ybarra, M L (2008), 'Online "Predators" and Their Victims: Myths, Realities and Implications for Prevention and Treatment', *American Psychologist*, 63(2), pp111-128.

[19] Ibid, p111.

© Becta 2008

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 young people more accessible to offenders and create opportunities for molesters to be alone with victims.[20] 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 non-forcible sexual activity with victims who are too young to consent to sexual intercourse with adults."[21]

Parents, schools and government do not generally make policy for children's protection by assessing known risks, but by imagining the worst that may happen and then guarding against it. 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 the UK, the Child Exploitation and Online Protection (CEOP) Centre was formed by the Home Office to work with police forces to track and bring offenders to account. In its Annual Review for 2007-8, CEOP states that, as a direct result of its activity, 25 of the UK's high-risk child sex offenders have been located, 131 children have been safeguarded and 297 arrests have been made.[22] No data is currently available on conviction rates.

In an increasingly risk-averse society, where schools have a duty of care to children and are vulnerable to legal action by parents, there is a strong incentive to try and prevent worst-case risk to children within their purview. For most schools, this currently means preventing children from engaging in any social activity on the web at school and tightly controlling the websites that they can access. 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 for society at large. 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. Thus, schools are faced with the dilemma of how to enable children to develop a mature approach to engaging with the internet, while exercising their legal duty of care.

It may help in exploring the difficulties faced by schools and policy-makers in regard to 'stranger danger' to refashion the central dilemma into a set of operational choices relevant to Web 2.0. Should schools and local authorities guard against the worst

[20] Ibid, p121.

[21] Ibid, p113.

[22] Child Exploitation and Protection Centre (2008), *Annual Review 2007-08*, London: CEOP, p9 [http://www.ceop.gov.uk/downloads/documents/ceopannualreview2008.pdf – accessed July 2008].

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 that prohibit 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[23] suggests that "posting personal information online does not, by itself, appear to be a particularly risky behaviour". 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 young people 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."[24]

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

Online bullying, or 'cyberbullying', can be an upsetting experience. A survey by Li[25] of 264 students from three junior high schools in Canada showed that almost half of the students were victims of bullying and about one in four had been cyberbullied. This percentage matched that from a smaller study conducted in London (though this

[23] Ibid, p117.

[24] Ibid, p117.

[25] Li, Q (2006), 'Cyberbullying in Schools: A Research of Gender Differences', *School Psychology International*, 27(2), pp157-170.

© Becta 2008

included phone calls and text messages).[26]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 calls, 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. 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 some parents insist on this so their children can contact them in an emergency. For some schools, accessing a proxy site (a means to access banned websites) is a disciplinary offence; in other schools studied, it was accepted or even encouraged by teachers as a means to bypass 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.

[26] Smith, P, Mahdavi, J, Carvalho, M and Tippett, N (2006), *An Investigation into Cyberbullying: Its Forms, Awareness and Impact, and the Relationship between Age, Gender and Cyberbullying – A Report to the Anti-Bullying Alliance*, Nottingham: DfES Publications.

© Becta 2008

Findings from the Becta Web 2.0 project related to e-safety

The Becta Web 2.0 project has carried out surveys of 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 report, we have combined data from both categories of school, except where otherwise specified, since the purpose of the document is to provide resources that assist in identifying issues and forming positions rather than to make comparisons or judgments.

Survey data

The survey data is from a questionnaire administered to 2,611 children in Years 8 and 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 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. Nearly three-quarters (74%) of the respondents report having used social network sites, with 78% sharing files on social networking sites occasionally or frequently.

Internet security

The respondents were asked direct questions to assess their use of instant messaging (IM) or email passwords (Table 1). Nine per cent indicated that they occasionally revealed their passwords to other people and 2% said they did so frequently. 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. Twenty per cent reported that they had occasionally learnt a password of another person, and 8% reported having done so frequently. Twenty-three per cent reported that they never changed their password, 37% did so rarely, 27% occasionally and 9% frequently.

© Becta 2008

Table 1: Learner's email/IM password security

	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 people's passwords	5%	31%	35%	20%	8%
I change the passwords I use	3%	23%	37%	27%	9%

The survey also asked respondents to suggest a password of at least six 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.

Table 2: Response to suggestion for a password

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%

Interactions with strangers

A series of items probed the pupils' 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 instant message from a stranger, and 14% had received such messages frequently. The data also shows 20% having occasionally sent an instant message in reply to a stranger, with 15% having done so frequently. A similar pattern is shown for email messages, though with lower rates of replying to strangers. Twenty-one per cent of the respondents indicated that they occasionally engaged in instant messaging or email correspondence with online

© Becta 2008

friends they had never met, and a further 17% indicated that they did so frequently. 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 they are inherently risky or not.

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

	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 [not including spam] from people I don't know	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%

As regards their use of social networking sites, 32% reported occasionally receiving requests to be friends from unknown people, with 22% receiving such requests frequently (Table 4). Twenty-nine per cent occasionally accepted such requests, and 22% accepted them frequently. Twenty-seven per cent reported occasionally maintaining online friendships with people they had not met in person, and 15% did so frequently.

Table 4: Social networking with 'people I have never met'

	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%

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 naive 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-

© Becta 2008

to-face friendships, involving friends of friends and people encountered in the online world, for example, through multiplayer games.

Online bullying

In reply to questions about inappropriate social network activity, 13% of respondents who used these sites reported that people had occasionally posted pictures of them that they wished had not been posted, with 3% reporting that this happened frequently (Table 5). Ten per cent reported that people had occasionally written unacceptable things about them online, with 3% reporting such behaviour happening frequently. 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. The slightly higher incidence of unwanted text-based postings at Web 2.0 innovating schools was not tied to a particular gender or year group.

Table 5: Unwanted postings of text and pictures

	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%

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 (130 teachers) and Web 2.0 schools (76 teachers). For the purposes of this report, we have not distinguished here between the categories of schools. 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. Nearly a third (30%) had uploaded a video they had shot, with 12% doing so as part of school activity.

© Becta 2008

Only 55% of teachers surveyed stated that their school had an e-safety policy, 3% believed that their school did not have such a policy, and 42% did not know. Forty-two per cent of teachers said they never taught students about e-safety, 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.

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

	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%

Online bullying

The main concern expressed by teachers was 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).

Table 7: Teacher response to 'bullying through online postings is currently a problem'

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

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, and discussing this with the pupils. Students were very aware of this incident. In focus group interviews with the students, the boys generally found it amusing, while the girls did not.

© Becta 2008

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 admitted responsibility when faced with the evidence and were 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 co-ordinator 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. 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 headteacher from Web 2.0 school)

This last quotation highlights the 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 mobile 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 this 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:

© Becta 2008

> "The [popular] argument is internet safety… [fears of] 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… you go onto some other websites and God knows what the kids access at home." (Teacher from Web 2.0 school)

A tension that frequently occurs 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 co-ordinator)

> "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 being cut off from the resources and interactions of the public internet. One view is that to

© Becta 2008

move outside the protection of a closed and moderated space is to expose children, teachers and the school to unnecessary risk; another view 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 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 indentified plagiarism (by copying text from websites) and cyberbullying 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 local authority. In a small number of schools, there was a lack of communication or understanding about how to unblock a desired site. According to teacher interviews, the time needed to unblock a site varied from a few minutes to a few weeks.

An overarching 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 naive 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.

Co-operative approaches

An indication of a co-operative approach to internet safety comes from a school where a few students had persistently broken through internet filters. Under the supervision of the ICT assistant head, the students were trialling new software, researching career paths and preparing presentations for governors. According to this member of staff, the subversion still happens but is "not malicious".

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. Over the last three, four

© Becta 2008

> years, we've got a fair number of websites that have been opened up, but they're all very much for educational use. So, I worked with the school council to put together a proposal to management that we would have open access to the web for pupils, and that would be two half-hour slots in the week. There's obviously a contract that they've got to sign beforehand, and they realise that not everybody can just come and descend on one room to get access… 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 suggest they have a better understanding of technology than their children: only 13% report that they know less about computers and technology than their children. Table 8 illustrates how some of these concerns are represented among 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 websites (13% strongly agree, 55% agree).

© Becta 2008

Table 8: Parents' opinions about risks involved in children's use of technology

	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 websites 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%

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. Ninety-one per cent 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 IM 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 (Table 9).

© Becta 2008

Table 9: Parents' opinions about children's online safety behaviour

	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%

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 30 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 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[27] 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).

[27] See http://is.njit.edu/pubs/delphibook/ch3b1.html for an authoritative introduction to Policy Delphi.

© Becta 2008

Figure 1: A 'dimension of difference' from the Policy Delphi workshop

Individual---------- Community

Δ

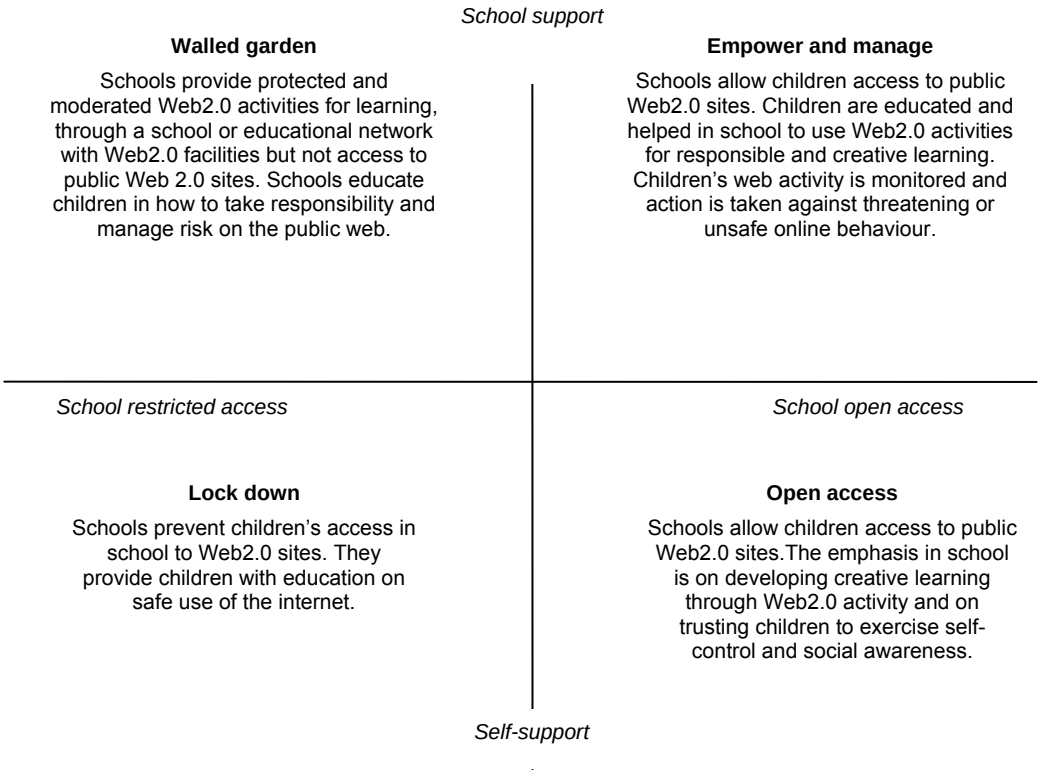
Responsibility

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.

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.

© Becta 2008

Figure 2: Policy positions produced from the 'dimensions of difference'



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, while '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

© Becta 2008

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 at Key Stages 3 and 4 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.

Table 10: Results of the ranking exercise for four policy positions on Web 2.0 and e-safety from the advisory panel

	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

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 who advocated open access indicated the need for moderation:

© Becta 2008

> "[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 and 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 gardens also stop students from exploring sites and developing their own personal ideas of what is appropriate or 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

© Becta 2008

> 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."

© Becta 2008

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 virtual learning environment, 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. This balance is well expressed in *TheChildren's Plan*:

> "Keeping children and young people safe from harm must be the priority and responsibility of us all. However, children need also to be able to learn, have new experiences and enjoy their childhoods, so we

© Becta 2008

> will help families strike the right balance between keeping children safe and allowing them the freedom they need."[28]

In relation to Web 2.0 implementation in schools, the advisory 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. These concerns are being addressed by the implementation of the Byron Review and should provide a context for development of appropriate access to Web 2.0 in schools.

Although the panel members, with one exception, did not support the development of a 'walled garden' of educational Web 2.0 services at Key Stages 3 and 4, 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

[28] Department for Children, Schools and Families (2007), *The Children's Plan: Building Brighter Futures*, London: HMSO.

© Becta 2008

understanding their development is to court failure… negative criticism must be accompanied by constructive efforts."[29]

[29] Bauchard, P (1953), *A Report on Press, Film and Radio for Children*, Paris: UNESCO, p14.

Resources

Schools

Schools section of Becta website
http://schools.becta.org.uk/index.php?section=is
Offers advice and guidance for keeping children safe online.

Signposts to Safety: Teaching E-safety at Key Stages 3 and 4
http://publications.becta.org.uk/display.cfm?resID=32424
Aimed at classroom practitioners, it contains background information, advice and guidance for teachers relating to safety issues and signposts appropriate opportunities within the ICT, PSHE and Citizenship curricula where internet safety messages can be taught. Additionally, it signposts free online teaching resources from a range of organisations to help support lessons.

E-safety: Developing Whole-school Policies to Support Effective Practice
http://publications.becta.org.uk/display.cfm?resID=25934&page=1835
This publication provides guidance for schools on developing appropriate policies and procedures to ensure safe use of communications technologies by the children and young people in their care. It outlines the risks, suggests an educational framework for schools, and gives an overview of the internet safety responsibilities of all the key stakeholders in a child's education. It provides practical strategies to follow, drawn up in consultation with the police, should major problems be encountered.

Local authorities and local safeguarding children boards

Safeguarding Children Online: A Guide for Local Authorities and Local Safeguarding Children Boards
http://publications.becta.org.uk/display.cfm?resID=31049
This publication contains a series of practical checklists for local authorities and more specifically for the newly formed local safeguarding children boards (LSCBs) for developing a co-ordinated approach to e-safety across all services under its remit.

Safeguarding Children Online: A Checklist for Local Authorities and Local Safeguarding Children Boards
http://publications.becta.org.uk/display.cfm?resID=31051
This summary publication contains a series of practical checklists for local authorities and more specifically for the newly formed local safeguarding children boards for developing a co-ordinated approach to e-safety across all services under its remit.

Safeguarding Children in a Digital World: Developing an LSCB E-Safety Strategy
http://publications.becta.org.uk/display.cfm?resID=35446&page=1835

This publication has been designed as a toolkit to support local safeguarding children boards and local authority personnel develop an e-safety strategy. It comprises suggested guidance (including strategy contents), outlines personnel who should be involved and aspects that should be covered. Case studies, activities and exemplar materials provided by local authorities help to illustrate practical steps to take.

Strategy and policy-makers

Safeguarding Children in a Digital World; Developing a Strategic Approach to E-safety
http://publications.becta.org.uk/display.cfm?resID=25933&page=1835
This publication provides a strategic overview of e-safety issues to policy-makers and outlines a model for a co-ordinated approach by all of the key stakeholders.

Research

E-safety: The Experience in English Educational Establishments
http://www.becta.org.uk/research/reports/esafetyaudit
Becta commissioned this research in August 2005 to audit the current level and range of activity within English state-maintained educational establishments to ensure the safe and effective use of ICT. The research was led by Charlotte Barrow from the Department of Education and Social Science at the University of Central Lancashire. Both the full report and executive summary and recommendations can be downloaded.

All

Safetynet Discussion Forum
http://lists.becta.org.uk/mailman/listinfo/safetynet
Safetynet is a mailing list for anyone who wants to discuss and share information to support the development of e-safety good practice within educational organisations. This forum is for teachers and others who have an interest and/or responsibility in this area. It has been set up to provide:

- peer-to-peer support and access to the shared knowledge and experience of the community
- instant access to colleagues, some of who may have similar difficulties and concerns
- access to help from other experienced practitioners and interested parties
- up-to-date information.

© Becta 2008

Other resources

CEOP
http://www.ceop.gov.uk
http://www.thinkuknow.co.uk

Childnet International
http://www.childnet-int.org
http://www.digizen.org

Directgov
http://www.direct.gov.uk/en/Parents/Yourchildshealthandsafety/Internetsafety/index.htm

Ofcom
http://www.ofcom.org.uk/advice/media_literacy

Home Office
http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

© Becta 2008