Sheffield Hallam University

Improving e-safety in primary schools: a guidance document

Final Report

Lucy Shipton

September 2011

Centre for Education and Inclusion Research
Sheffield Hallam University

Contents

Centre for Education and Inclusion Research
Sheffield Hallam University
Unit 7 Science Park
Howard Street
Sheffield
S1 1WB
Tel: 0114 225 6060
Fax: 0114 225 6068
e-mail: **ceir@shu.ac.uk**
www.shu.ac.uk/ceir

Policy context

Major developments have taken place in recent years around safeguarding and children's services[1], and subsequently the safeguarding of children has moved up the political agenda. An important part of the focus on safeguarding has been around children and young people's use of digital technology and their e-safety.

The development and use of digital technology has grown quickly, and advancements in social networking sites, web-cams, portable media devices, and online gaming have been particularly appealing to children and young people. Whilst these technological developments bring benefits and opportunities to children and young people in terms of their learning and development, they also bring about safeguarding implications.

E-safety risks to children have arisen in relation to cyber-bullying, the invasion of privacy, accessing inappropriate materials such as pornography, and communicating with strangers. A survey on young people's internet safety by YoungPoll (Childalert, 2011) found that the average 6-14 year old communicates with more than 1,100 people online in a year, that over a quarter never spoken to their parents about how they spend their time online, of those who had, less than half had discussed e-safety, and that only 34% had met in real life all the people they communicated with on the internet.

Two independent reports were commissioned by the Government to look at children and new technology and the risks they face online (Byron, 2008, 2010). The first of these reported that:

> *...there are concerns over potentially inappropriate material, which range from content (e.g. violence) through to contact and conduct of children in the digital world (Byron, 2008 p2)*

Byron suggested a shift away from the viewpoint that new technology causes harm to children and young people towards an understanding around how they can be empowered to manage the risks. The initial report set out a national strategy for the Government, industry and families to work together to help keep children safe online, and also made a number of recommendations including:

- a focus on e-safety in schools through the identification of e-safety as a national priority for CPD (Government);
- a move towards holding schools to account in terms of their e-safety practices and the consideration of an assessment of e-safety performance in school inspection reports (Ofsted);
- ensuring new teachers have e-safety knowledge and skills (TDA); and
- the regular review of Acceptable Use Policies (AUPs) in schools that are agreed with parents and students and use an accredited filtering system (schools).

[1] For example, *Safeguarding Children Report* (2002); *The Laming Report* (2003); *The Every Child Matters programme* (2004)

In 2007 Ofsted introduced a question to the self-evaluation form asking about the extent to which pupils adopted safe and responsible practices when using digital technologies. In response to Byron's 2008 review Ofsted carried out a small evaluation of 100 school self-evaluation forms, and found that there were significant differences in the ways schools assessed and monitored their e-safety policies. This was a particular issue in primary schools. Further concerns were found around the level of cyber-bullying, along with how to deal with it and the school's responsibilities when it extended beyond the school day. Most schools had blocked access to social networking sites and instant messaging services in an attempt to eradicate their cyber-bullying problems. The evaluation recommended that self-evaluation forms continued to include references to e-safety and that Ofsted inspectors should receive appropriate training and guidance around the issue.

Following this, in September 2009 Ofsted introduced a new school inspection framework which included a stronger focus on safeguarding and e-safety. The evaluation schedule for schools (Ofsted, 2010a[2]) included the following statements around e-safety and safeguarding in schools which inspectors are required to take into account:

- the school *'has clear policies, strategies and procedures to ensure the safeguarding and welfare of pupils';* p50
- *'the effectiveness of the school's arrangements, including links with key agencies, for ensuring the safety of its pupils';* p50
- the school *'ensures that adults receive up-to-date, high quality, appropriate training, guidance, support and supervision to undertake the effective safeguarding of pupils'* p50
- the school *'monitors and evaluates the effectiveness of its policies and practices'*; p50
- the school takes into account of *'the extent to which pupils are able to understand, assess and respond to risks, for example those associated with new technology'*; p17
- the school '*helps pupils to keep themselves safe, including encouraging pupils to adopt safe and responsible practices and deal sensibly with risk...[using the internet]'* p50

The importance of e-safety has been amplified through these changes, and any schools receiving a grade 4 or inadequate for its safeguarding arrangements are now likely to obtain a grade of 'inadequate' for their overall performance.

In 2010 Ofsted followed up these changes with a *Study of the Safe Use of New Technologies* (2010c) to evaluate the extent to which schools teach pupils to adopt safe and responsible practices in relation to digital technologies. The study found that there were a number of factors that led to a school being 'outstanding' in e-safety, these included:

- having an active approach;
- a close relationship between provision and pupils' knowledge and understanding;

[2] http://www.ofsted.gov.uk/resources/evaluation-schedule-of-judgements-for-schools-inspected-under-section-five-of-education-act-2005-sep

- well established staff training which was monitored and evaluated;
- well planned and coordinated curriculum;
- using 'managed' rather than 'locked down' systems;
- systematic reviewing and evaluation of e-safety policies;
- shared responsibility for provision;
- leaders, governors, staff and families working together to develop a clear strategy;
- excellent relationships with families; and
- systematic training of staff.

Byron's second review (2010) looked at the progress that had been made since 2008 and found that there had been significant improvements in relation to children's safety. The report agreed with Ofsted's suggestion that schools use managed rather than locked down systems[3], deeming the latter to be an ineffective way of helping children and young people to independently manage their own safety:

> *…simply blocking children and young people's access to the internet in schools…meant that they weren't able to access a range of sites that were beneficial for learning, and that they were less likely to develop the understanding of digital safety that they needed to be digitally safe outside of school* (Byron, 2010 p16)

Byron suggested that Ofsted's recommendation around schools moving towards more managed systems and fewer inaccessible sites should be supported by the UK Council for Child Internet Safety (UKCCIS).

In terms of improving education, Byron (2010) reported that progress had been made around incorporating e-safety into the curriculum[4], stressing that this needed to be embedded across the curriculum and not confined to a single subject such as ICT or PSHE. Significant advances were also noted in relation to initial teacher training in digital safety, with a TDA survey (2009) stating that 77% of newly qualified teachers felt they understood the risks that children and young people faced in relation to e-safety and 74% believed that they could use this knowledge in their teaching practice. However, there is still more that can be done in terms of training all school staff in digital safety and not just newly qualified teachers, and this has been reflected in Byron's suggestion for NCSL and Children's Services to develop her 2008 recommendation to support school leaders to prioritise e-safety CPD for school staff.

Byron noted important improvements in the development of resources and materials for schools and teachers, school policies, and inspections. With schools now being more able to access comprehensive advice on their digital provision and e-safety policies, for example through Becta's published guidance on the development of effective AUPs, and digital safety now being included in Ofsted's judgement of schools in their grade descriptor for *'effectiveness of safeguarding procedures'*.

The remainder of this document outlines the findings from two case studies carried out by the Centre for Education and Inclusion Research at Sheffield Hallam

[3] Locked down systems block access to certain websites on the internet whereas managed systems have fewer filters in place

[4] To come into effect in September 2011

University on behalf of the TDA in English primary schools in the summer term of 2011. The schools involved were felt to be more advanced in terms of their e-safety awareness than many primary schools, and the research sought to uncover what they had implemented, where they had been successful, and any barriers they had faced. The research is particularly pertinent due to the recent changes to the Ofsted inspection framework and the importance for schools to reach 'outstanding' in terms of safeguarding.

The research took place in a large primary school in a city in the north of England (School A), and a small rural Church of England primary school in the south west (School B), and included initial telephone interviews with the head teacher and fieldwork visits which involved interviews with: the head teacher; the teacher with a lead in e-safety; other teaching staff; and focus groups of children.

The Case Study Schools

School A

A very large primary school situated in a city in Yorkshire and Humber. The school is located in a catchment area with varying social circumstances covering both a private housing estate and council housing. Almost all pupils are of White British heritage and speak English as their home language. The proportion of pupils with special educational needs/disabilities is just below average as is the percentage entitled to free school meals. The school is federated to a secondary school which is located on the same site as the primary.

A minority of pupils at the school are very 'streetwise', and are known to hang around with older children on the streets at night. Many children have access to laptops and there are some issues in the school in terms of cyber-bullying, online arguments and the use of webcams. E-safety issues in school tend to originate from outside of school time and then spill into the classroom and playground.

Particular concerns have arisen in Year 3 where children have been known to bully each other online in Club Penguin and Habbo Hotel[5] and with very young children playing on age-restricted games such as Call of Duty. When asked by their teacher the majority of Year 6 children admitted to having a Facebook account[6], and the school is aware of a Year 2 child having an account. Parents generally feel that it is acceptable for their children to have a Facebook account, but the school believes that this sends out an inconsistent message.

[5] Club Penguin and Habbo Hotel are virtual communities for children and teenagers to play games and chat

[6] Facebook has age-restrictions in place, to register an account you must be 13 years old or over

School B

A very small rural Church of England primary school situated in the South West with mixed-age classes. The catchment attracts pupils from nearby villages who are predominantly from an affluent middle-class background. Almost all pupils are of White British heritage and speak English as their home language. The proportion entitled to free school meals is below average, and the proportion with special educational needs/disabilities is average. When pupils start at the school attainment is generally average or slightly above.

The school roll has doubled in the past 5 years, leading to the reorganisation of classrooms and internet connectivity issues where the school exceeds its limit on a daily basis. All pupils at the school have access to the internet both at home and at school, and generally spend around 2-3 hours a day online. Fizzbooks[7] have been provided for the older children in Years 4-6 due to their class relocation away from the ICT suite.

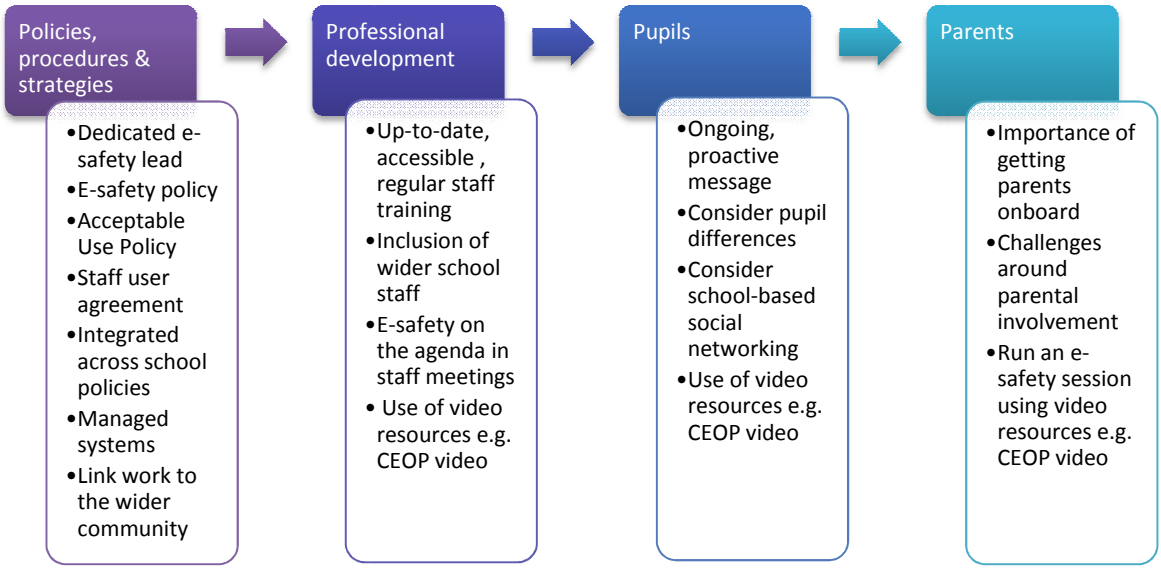
The main e-safety concern at the school is around social networking sites. Around 40% of the older children (Year 4-6) have Facebook accounts, some as young as seven years old. The rest of this age group are using MSN and text from mobile phones. Many parents at the school assume their children are not on social networking sites like Facebook due to the age restrictions. Concerns have arisen around how the children conduct themselves online with their friends and the safety risks in terms of social networking accounts.

Key messages in improving e-safety

The following section uses the findings from the two case studies to provide an overview of what works in terms of improving and raising e-safety awareness in primary schools, as well as the barriers and challenges schools may face in trying to implement them. Figure 1 below provides an overview of the research findings.

[7] A Fizzbook is a mini-tablet computer designed for children

Figure 1: An overview of improving e-safety in primary schools



Policies, procedures and strategies

The research revealed the importance of having a **member of staff with a lead role** in relation to e-safety in the preliminary stages of developing e-safety policies and programmes. The lead person should be someone with enough time to oversee e-safety and be IT literate. They should also consider building up their base knowledge by being up-to-date with current e-safety issues before attempting to develop an e-safety policy or cascade information down to the pupils.

The development of an **e-safety policy** is crucial to improving internet safety in schools. The head teacher from School B noted how putting together an e-safety policy had been made easier through reading relevant background literature such as the Byron Review and thinking about what it meant for them as a school.

The research showed that whilst schools were already using common sense in relation to any e-safety incidences that occurred, the development of a dedicated school policy had meant that any problems could be addressed quickly, with all members of staff being clear about what steps to take and if necessary who to escalate concerns to, seeing it as *"a set of guidelines to work to"* (School A, Teaching Assistant).

Schools should be aware that e-safety policies will need to be updated regularly due to the nature and speed at which concerns change in the digital world:

> *It's an ongoing thing...it's changing every day…you've got to keep going back to it, just to keep up-to-date with it* (School A, Teaching Assistant)

The case study schools noted how their policies had been enhanced through consultation with staff, governors, parents and pupils. The importance of involving parents in the development of an e-safety policy was noted during the research process because unlike most other school policies it affects children both within school and at home.

E-safety matters encompass many aspects of school life, and schools may therefore find it helpful to update other policies so as to include any relevant internet safeguarding issues. The research revealed a number of ways in which e-safety had been integrated into whole school policies, for example:

- Updating the Home-School Agreements
- Altering the priorities in the School Development Plan
- Changing the Positive Behaviour Policy to incorporate cyber-bullying

Schools should also take into account revisions to their **Acceptable Use Policies**, and consider the merits of them being updated on an annual basis so that any new digital concerns can be integrated. The case study schools pointed out the importance of this document being signed by pupils once a year, as well as it being sent home with an accompanying letter to support parents in keeping their children safe when using the internet at home.

The Acceptable Use Policies in the case study schools included rules and advice for children around:

- turning off the screen and informing an adult if they find anything unpleasant or disturbing online;
- touching files that are not their own;
- being respectful to other people online;
- sending abusive or inappropriate text messages;
- giving out personal details that might identify them or their location;
- placing photos of themselves online;
- denying access to unknown individuals;
- blocking unwanted communications; and
- privacy settings, security and passwords.

Comments were also made around the benefits of separate Acceptable Use Policies for Key Stage 1 and Key Stage 2 pupils, and the advantages of having them posted in classrooms with internet access as a constant reminder of what is acceptable.

Particular issues were found in the case study schools around children acting differently online than they would in the real world, the use of social networking sites without privacy settings, and the inclusion of a level of detail that could generate risks for the child.

When implementing e-safety modifications, schools may want to include a **Staff User Agreement,** which outlines what is appropriate and professional for staff in terms of their online behaviour. Both case study schools had implemented such an agreement, advising staff not to set social networking privacy settings so that pupils could access their accounts:

> *[Staff should be]…cautious of information shared on social network sites and be mindful of who has access to this information and the importance of good security settings* (School B, Staff User Agreement)

This was a particular issue for Case Study School A where many staff members lived in the local community, knew the pupils outside of school, and had links with them through Facebook.

Schools may also want to consider how they want to address e-safety at an organisational level, taking into account the management of information systems[8], the school website (such as the inclusion of personal information about staff or pupils and identifiable images), and the level of filtering used.

The case study schools advocated **managed systems** with fewer filters in place rather than locked down ones, as it was felt that they assisted children in managing online risks rather than avoiding them at school and being exposed to them elsewhere. One school spoke about their Managed Learning Environment (MLE) which included an area around e-safety where children could report anything they were unhappy about or uncertain of. Links to e-safety websites such as CEOP[9] were also included on the MLE so as to give children more information which they would hopefully share with their parents/carers.

The other school had a filtering system in place which had been set by the local authority, but felt this was problematic as the blocked sites were ones that the children could freely access at home:

> *I think it would be far better if the children could access more and we could teach them how to use it properly, and have systems in place if things went wrong. I think it would be much more like the real world, because children can access a lot more at home, and if they could access it at school we could teach them to use it appropriately, it would be much better. The only way you can do that [here]…is by taking over all responsibility for the ICT, and schools are really quite reluctant to do that, and I can understand why...at least it's safe, and you don't have to worry about what might be accessed, but I don't think it's preparing them very well for what they might be accessing at home* (School B, Head teacher)

Once systems are up and running internally, schools may want to consider incorporating their learning around e-safety into the wider community. One of the case study schools had started to build links with the federated secondary school, local primary schools and breakfast and after-school club leads in terms of e-safety for the ICT they use in wrap-around provision.

Professional development and training

Once the policies, procedures and strategies have been developed, schools should consider getting the rest of the staff base onboard by explaining the importance of e-safety and organising training around their own safe and responsible use of the internet and the school's e-safety policies.

Training should be **up-to-date and accessible** to ensure that all staff - whatever their level of awareness around digital technology and e-safety - are knowledgeable about the implications for pupils in their school. Discussions around the general principles of e-safety as well as what steps to take if an e-safety issue arises could be included, along with explanations of why schools should be interested in e-safety in pupils' homes:

[8] In terms of updating virus protection, the encryption of personal data and the Data Protection Act.
[9] The Child Exploitation and Online Protection (CEOP) Centre is a UK policing unit dedicated to eradicating the sexual abuse of children.

> *…in the same way that if you hear about children's welfare in other ways you need to pay attention to it and act upon it* (School B, Head teacher)

In one of the case study schools, the teacher with the lead role in e-safety attended a local course where she gained a more in-depth understanding of the issues surrounding specific sites such as Facebook, Bebo, Club Penguin and Habbo Hotel. The training was then rolled out by the lead teacher for all classroom staff (including training assistants), and then to all staff including those in support roles and governors. The other school, which was located in a rural setting, had found difficulties accessing external high quality training, and had subsequently organised the initial training themselves.

An online video by the CEOP[10] was used by both of the case study schools as part of their staff training, and was felt to have had a big impact in terms of embedding the issues around e-safety for primary school aged children.

Schools should also take into account **the inclusion of the wider school staff**[11] in e-safety training, especially in relation to their links to children on social networking sites[12]:

> *100% of the staff have been involved in the training...the impact on the staff has been huge* (School B, Head teacher)

In larger schools, such as Case Study School A, it may be easier to break down the training, with teaching staff taking part first and then rolling it out to the wider staff group.

The research findings revealed the importance for staff training to be part of a rolling programme due to staff turnover and the speed at which new concerns crop up in the digital world. In addition to this e-safety updates may be included as a regular feature in staff meetings, so that issues and updates can be discussed as and when they arise.

Getting the message across to pupils

Once policies, procedures and strategies are in place and staff are trained and aware of the school's e-safety requirements the next step is getting the message across to pupils. Schools should consider taking a proactive approach in terms of informing their pupils about e-safety, preparing them beforehand rather than reacting to situations as they arise.

E-safety messages should be **ongoing**, perhaps starting with some dedicated time to embed it, and then integrating it into everyday life in the school. ICT is used across the curriculum and therefore the e-safety message can be reinforced across the majority of lessons, with it also being revisited on a regular basis perhaps through circle time, ICT or SEAL.

[10] https://www.thinkuknow.co.uk/teachers/resources/
[11] Catering assistants, lunchtime supervisors, office staff and cleaners for example
[12] More around this is outlined above in the policy section

Before developing a plan around how to deliver e-safety awareness to children, schools may want to consider **pupil differences**. Pupils in a certain year group in one school may not be at the same level in terms of maturity or be as 'street-wise' as those in another school; this may even be the case between different cohorts of children within the same school. One of the case study schools had found benefits in carrying out a questionnaire with their children before implementing their own teaching around the subject. This gave them an overview of what the children were aware of in terms of the internet and e-safety, and gave them an indication of what needed to be addressed. Schools should note the importance of discussions being pitched at the right level by making them aware of the risks and dangers, but not scaring them unnecessarily.

The case study schools both used the same CEOP video with their children as an e-safety starting point. The age-restricted video is for 8-10 year olds and shows children the dangers of social networking sites in terms of privacy settings, speaking to strangers, cyber-bullying and putting photos online. Teachers from both schools felt the video had quite a strong message and was hard-hitting but felt it needed to be like that to make the children take note. Children from both schools spoke about how they had made changes to their Facebook accounts after watching the video.

The case study schools had both started their initial e-safety work with the older children in the school and were planning on working with the younger ones (albeit in a different format) in the coming year. The enormity of implementing e-safety changes had meant it had been difficult for the schools to get the message across to all pupils at once, but both indicated that it needed to be addressed before they reached the upper end of the school, as by this time they were already making use of digital technology and were unaware of the risks they might be taking. The schools felt confident that once the whole e-safety programme was in place they would be able to teach the children about e-safety from the point they entered the school and therefore prevent any unnecessary online risks.

One school had carried out some initial work with the younger children through an online resource called Hector's World[13]. The website is designed to encourage safe online behaviour for 2-9 year olds and '*promote the skills and values young people need to grow into confident, knowledgeable and caring members of the online community*'[14], through the adventures of Hector the dolphin and via lesson plans and classroom activities. Through this the children had learnt to shut down the computer if they came across anything inappropriate and to tell an adult.

Schools may also **consider using school-based social networking sites** such as Edmodo[15] which can help train children in a child-friendly way for when they inevitably move on to sites like Facebook. Edmodo enables the teacher to have an overview of what is being posted and monitor any inappropriate online behaviour. Groups can be set up so that children are only in contact with other people in their year group and it can be used either within the classroom or from home. One of the case study schools had introduced Edmodo as part of a topic around space, where an alien had landed in the school and was on the site answering the children's

[13] http://www.hectorsworld.com/island/index.html
[14] http://hectorsworld.netsafe.org.nz/teachers/
[15] http://www.edmodo.com/

questions. The children at the school talked about how it had taught them to post comments appropriately, how they had felt safe as they knew no-one could hack into the site, and how they could report anyone that had upset them on there.

Once the initial messages have been conveyed through dedicated e-safety sessions, the Acceptable Use Policy can be explained and then signed by the pupils. Schools may find it helpful to post the rules and advice from this policy in any rooms with internet access.

Getting the message across to parents

E-safety differs from many areas that schools deliver in terms of the links it has with the community and home. Schools should therefore consider whether e-safety messages being given within the school should be reinforced in those arenas outside of school where children are also accessing the internet, such as at home.

The case study schools felt that **involving parents is incredibly important**, as this helps to ensure the children are hearing a consistent message around e-safety. They attempted this through a number of methods such as drawing their attention to the new e-safety policy via newsletters, the school website and the prospectus, asking them to co-sign their child's Acceptable Use Policy document, and organising training sessions where the parents could view the CEOP video and discuss their e-safety concerns.

However, both schools faced **challenges in trying to get the message across to parents** and carers. One school had found parental perceptions of e-safety to be very different to those held in the school, and were aware of many parents who had created Facebook accounts for their children using fake dates of birth:

> *The problem is you do your bit in school and you give the message out and we reinforce constantly…and they go home and a difference message is given, and obviously what their parents say has the bigger sway* (School A, Head teacher)

Often these parents felt that because their child was in the same room as them whilst using the internet that they were safe. Parents from this school pointed out that e-safety issues could arise on children's sites like Moshi Monsters[16], reinforcing the importance of teaching children to be safe online and equipping them with the knowledge to manage the risks safely.

Teachers from the other case study school noted how many of their parents were unaware that their children were accessing age-restricted sites, and although there were unusually high levels of engagement with their parents in terms of attendance at parents' evenings, school productions and family learning weeks, when it came to trying to engage them with the e-safety agenda they had had little success. They had tried to run an **e-safety session** for parents where they were planning on showing them both the CEOP video they had shown the children and another one aimed at secondary age children, but only one parent had wanted to attend. The school was

[16] Moshi Monsters is a free online game for children where they can adopt and look after a monster, make friends with other owners and leave messages on their pages

planning on re-running the parent training after the summer and giving it a much higher profile.

> *The biggest challenge has been getting parents to understand…Quite a few of them just close down on it, either ignore it and think it's just a child thing… some of the just don't want to know. That's the hardest I think it's going to be… That is a concern, parents is the biggest [challenge]* (School B, Teacher)

The head teacher felt there may have been problems with the timing of the event, but felt that the biggest challenge was due to a fear from parents and a trust that the school would be able to keep their children safe. Schools therefore need to be aware of the challenges in creating e-safety links between school and home:

> *This element of bridging the gap between home and school is a first for us, because we've always separated the two, ICT in school has been our responsibility, and we've always known our children have ICT access at home...but we've never held ourselves responsible for it (*School B, Head teacher)

This is even more important for hard-to-reach parents who are even more unlikely to attend training sessions or read information around e-safety in newsletters or on the school website.

Schools may also like to consider using children to deliver the e-safety message to parents, one of the case study schools felt that this would be a far more powerful way of disseminating the information to them. The head teacher spoke about how they were planning on putting together a short film around e-safety with their children presenting the message, which they would then place on their MLE so that parents would be able to access it from home:

> *...the children film the articles, edit them, we have the green screen…within the school....the e-safety thing is something we can use with the children to children, but also children to parents, because that's a really powerful tool....a bit of a backdoor way really…and even if you only get to a few where you're saying 'do you realise that you need to be 13' if it's a child delivering that message it's always far more powerful* (School A, Head teacher).

Initial impacts

The two case study schools are both in the early stages of implementing measures to improve e-safety and raise awareness for their pupils, and although they have many plans still to put in place the research revealed a number of impacts which had been felt already.

Impacts on schools

1. Far more advanced than they had previously been in terms of e-safety and felt they would definitely get an 'outstanding' in the safeguarding element of their next Ofsted inspection.
2. Higher e-safety profile

> *I think we'll be outstanding...we are much much better now than we were... the questions they might ask, we're in a much better position to answer them* (School B, Head teacher)

> *We can talk with clarity and it's part of the policy, it's in the School Development Plan, it's there. The strategic link is now within the development of the school, whereas before it was in, but it was an add on. So I feel much more confident now about how that works and where we are with it* (School A, Head teacher)

Impacts on staff

1. Better awareness amongst staff
2. Staff having the confidence to deal with e-safety concerns and incidents
3. Staff more likely to feedback any e-safety concerns and discuss them with colleagues
4. The CEOP video had had a bigger impact than anything else on staff and the schools were eager to show it to parents

> *The video has had a real impact on them [the children] and the staff...I think they are much more aware, and that's why I'm trying to get the parents in to see that video* (School B, Head teacher)

Impacts on pupils

1. Better awareness amongst pupils
2. Pupils knowing what to do if they see something inappropriate online
3. Improved online research skills amongst pupils (e.g. now know how to filter and use the internet appropriately)
4. Pupils were knowledgeable about not putting personal information online such as their phone number or address
5. Pupils were aware of what to do if someone sent them an inappropriate message, and not to send the message on to someone else
6. Since the CEOP video many pupils had set their social networking accounts to private, were not accepting friend requests from people they did not know, and removed photos of themselves

7. The CEOP video had had a bigger impact than anything else on pupils
8. Pupils approaching teachers far more often to report e-safety incidents or concerns
9. Pupils making less unkind comments to each other online, and knowledgeable about cyber-bullying
10. Pupils knowing what to do with spam and viruses
11. Pupils feeling safer online than they had done previously, both at home and at school

> *Whoever made up e-safety, I'm glad they did it because I now feel safer on the computer, at school and at home and wherever I go (School A, Year 5 pupil)*
>
> *[I've made] a lot of changes...my pictures are still up there but they are more less detailed photos, privacy settings are private, my teacher was really pleased, because she looked up my name on Facebook and it came up but then the next day I'd changed it and she couldn't get on it, so she was quite pleased (School B, Year 5 pupil)*
>
> *If over the social networks if someone says meet up and you don't know who it is, or someone requests you as a friend, just don't do it because they could be anyone (School A, Year 5 pupil)*

Impacts on parents

1. Parents were more likely to approach the school regarding e-safety issues
2. Parents acknowledged their children had become more internet savvy since learning about e-safety at school

> *There's not a lot the school can do if the parents just let them do what they want to do at home, we can only do for our kids and make our kids aware of it...we've had a couple of things sent home saying watch what your children are on and things, but I think it should be more or less instilled in them saying 'this is what could happen'* (School A, Parent)
>
> *I'm sure if they had that session that we had [CEOP video], it would really make an impact, it would make some of them sit up and think 'I've actually got to take this on board, I'm going to have to do something about it', not just assume that everything's fine* (School B, Teacher)

Strategic recommendations primary schools

Table 1 below is a checklist outlining issues for primary schools who are looking to improve e-safety to consider.

Table 1: checklist of e-safety recommendations for primary schools

	Definitely in place	Needs review and attention	Not in place
A dedicated e-safety lead			
An e-safety policy which is regularly updated			
Acceptable Use Policy for pupils			
A staff user agreement			
E-safety integrated across school policies			
Managed systems			
Up-to-date regular staff training			
E-safety as an agenda item in school meetings			
Training for all staff groups			
A proactive and ongoing approach to getting the message across to children			
E-safety pitched at the right level for children in the school			
Show the CEOP video to pupils, staff and parents			
E-safety work linked to the wider community			
Parents onboard with e-safety work			

References

Byron, T (2008) Safer Children in a Digital World: the report of the Byron Review. Nottingham: DCSF publications.

Byron, T (2010) Do we have Safer Children in a Digital World?: review of progress since the 2008 Byron Review. Nottingham: DCSF publications.

Childalert (2011) *How to Keep Children Safe Online.* Viewed 26 August 2011. http://www.childalert.co.uk/article.php?articles_id=206

Laming (2003) The Victoria Climbié Inquiry Report. Norwich: HMSO.

Ofsted (2008) School Self-evaluation: a response to the Byron Review. Manchester: Ofsted.

Ofsted (2009) School Inspection Framework. Manchester: Ofsted.

Ofsted (2010a) The Evaluation Schedule for Schools. Manchester: Ofsted.

Ofsted (2010b) Briefing for Section 5 Inspectors on Safeguarding Children. Manchester: Ofsted.

Ofsted (2010c) The Safe Use of New Technologies. Manchester: Ofsted,