guidance for leaders

Becta

improving learning
through technology

safeguarding children online

a guide

for Local Authorities and Local Safeguarding Children Boards

contents

about this booklet

Since 1998, in conjunction with the Department for Education and Skills (DfES) Becta has been providing advice and guidance to schools and local authorities (LAs) on all aspects of e-safety. Recognising that e-safety is not just the responsibility of practitioners, Becta has also been keen to promote the role of infrastructure and policy in e-safety.

In recent years, Becta has convened the Safe Use of ICT in Education (SUICT) Advisory Group to lead the debate on e-safety issues, with representation from key education and child welfare organisations (see page 28 for membership). It is from the work of this group that this publication stems.

Please note: This booklet does not intend to cover the specifics of e-safety issues or technologies. You will find those in previous Becta e-safety publications, many of which we have referenced here.

Where we use the terms 'e-safety' or 'online', we refer to all fixed and mobile technologies that children and young people may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks to their wellbeing and safety.

In its recent publication, *Safeguarding children in a digital world: Developing a strategic approach to e-safety*[1], Becta sets out for policy makers a strategic overview of e-safety issues. Through a series of recommendations, the publication outlines a model for a co-ordinated approach to developing an e-safety strategy that draws together policies and practices, education and training, and infrastructure and technology – all underpinned by inspection and standards.

This booklet, which builds on that guidance (and should therefore be read in conjunction with it), contains a series of practical checklists for LAs and more specifically for the newly formed local safeguarding children boards (LSCBs). By giving prompts, recommendations and signposts to useful resources, this booklet will help core members of LSCBs to develop and follow best practice in safeguarding from e-safety risks all the children in their care.

We hope that you will find it useful.

[1]See Becta website [http://www.becta.org.uk/corporate/publications/documents/BEC6189 Safegd Children AWLR.pdf]

LSCBs and e-safety – the issues considered

The statutory context for e-safety

Following on from the 2003 Green Paper *Every child matters*[2] and the provisions of the Children Act 2004[3], *Working together to safeguard children*[4] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

Every local authority has now established a local safeguarding children board as *the key statutory mechanism for agreeing how the relevant organisations in each local area will co-operate to safeguard and promote the welfare of children, and for ensuring the effectiveness of what they do*. *Working together to safeguard children* further defines the ongoing role of LSCBs, once their core business is in order, as follows:

3.3 The work of LSCBs is part of the wider context of children's trust arrangements that aim to improve the overall wellbeing (ie the five *Every child matters* outcomes) of all children in the local area.

3.4 While the work of LSCBs contributes to the wider goals of improving the wellbeing of all children, it has a particular focus on aspects of the 'staying safe' outcome.

The 'staying safe' outcome includes that children and young people be:

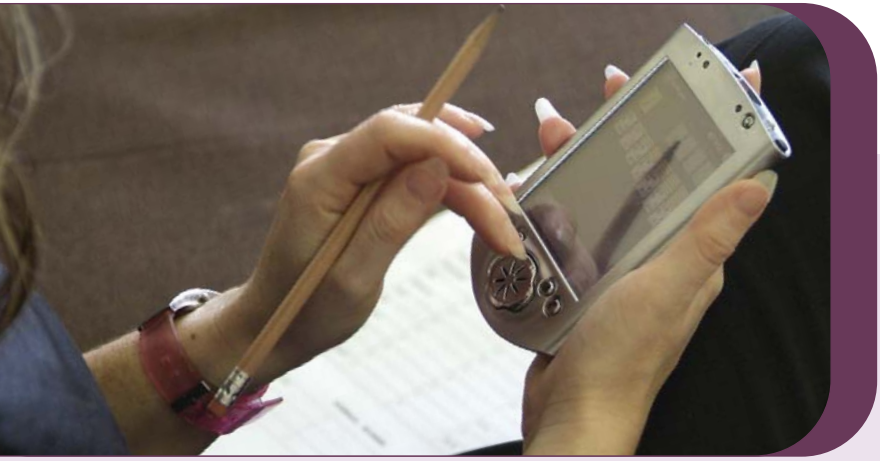
- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

It is here that the context for e-safety emerges.

[2]See the Children Act 2004 [http://www.opsi.gov.uk/acts/acts2004/20040031.htm]

[3]See Every child matters website [http://www.everychildmatters.gov.uk]

[4]*Working together to safeguard children: A guide to inter-agency working to safeguard and promote the welfare of children*, available on the Every child matters website [http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf]



Although undoubtedly these aims were written with the 'real world' in mind, many equally apply to the 'virtual world' that children and young people may encounter when they use ICT in its various forms. Indeed, for many young people, the online world is very much their reality – offering them unprecedented opportunities to communicate, create, discover and be entertained in a virtual environment.

However, we know that people have used the internet for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which has sometimes led to their involvement in crime and anti-social behaviour.

To ignore e-safety issues when implementing statutory guidance could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable. Non-statutory practice guidance issued in *Working together to safeguard children* includes a section on child abuse and ICT (paragraphs 11.58-11.62). Paragraph 11.62 states:

As part of their role in preventing abuse and neglect, LSCBs should consider activities to raise awareness about the safe use of the internet. LSCBs are a key partner in the development and delivery of training and education programmes, with the Child Exploitation and Online Protection Centre (CEOP). This includes building on the work of Becta, the Home Office and the ICT industry in raising awareness about the safe use of interactive communication technologies by children.

This clearly sets the context for why LSCBs must be concerned with e-safety. The following sections pose key questions for LSCBs, the answers to which will help them to formulate effective local policies, as well as to review and keep those policies up to date with today's rapidly changing online environment.

The extent of e-safety issues

Becta's publication *Safeguarding children in a digital world: Developing a strategic approach to e-safety*[5] outlines the issues and risks which children and young people face in relation to e-safety. Broadly, these factors consist of exposure to content, contact and commerce, along with cultural issues which might affect their wellbeing.

However, LSCBs must consider e-safety in the wider context, which includes access to ICT and the types of that access; they must also take into account the types of connectivity and the kinds of data and communication used.

Access to ICT

LSCBs must consider the range of access points to ICT across the full range of services under their remit. This may include schools, libraries, children's homes, Sure Start children's centres, youth clubs, and non-mainstream education settings such as hospital schools.

Each of these access points may face different issues in terms of the user groups they serve, the e-safety issues they face, and extent of the technical security they can implement. E-safety policies and practices will need to reflect individual circumstances.

LSCBs should also consider their role in promoting e-safety in the home. Research shows that home access to ICT continues to grow, with 60 per cent of all households in the UK[6] now having access to the internet. Additionally, initiatives such as Computers for Pupils[7] aim to put computers into the homes of disadvantaged secondary children to help improve their education and life skills as well as to benefit the whole family. LAs will administer the scheme, and it is estimated that over the next two years around 100,000 families will benefit from this scheme alone. Under their general duty of raising awareness, therefore, LSCBs will increasingly need to look for opportunities for advising parents and carers on the safe use of technology in the home.

[5]See Becta website [http://www.becta.org.uk/corporate/publications/documents/BEC6189 Safegd Children AWLR.pdf]

[6]Ofcom (2006) *The communications market 2006*, available online [http://www.ofcom.org.uk/research/cm/cm06/main.pdf]

[7]See the Becta website [http://www.becta.org.uk/schools/computersforpupils]

Types of access

There are many methods and devices for accessing the internet and online services, and their availability to children and young people is increasing. Modes of access include desktop and laptop computers, mobile phones, other handheld devices such as personal digital assistants (PDAs) and interactive games consoles, both fixed and handheld.

Although it may be impossible to control access across all these devices, every LSCB should consider its role in educating children and young people, through the services under its remit. If children and young people can learn to become safe and discriminating users of technology, wherever and whenever they use it, they will be better placed to protect themselves from the risks and challenges they may encounter.

Types of connectivity

Following on from the increase in access devices, connectivity to the internet and online services is no longer restricted to landline or broadband connections from a fixed location, but is using wireless technology to become increasing mobile.

Again, this limits the technical controls that can be imposed, meaning that effective e-safety education has a more important role than ever to play in safeguarding the welfare of children and young people.

Types of data and communication

Methods of e-communication are many and varied, and include text and digital images, both still and moving. No longer are children and young people merely recipients of content published on the internet: they have become active participants in the online world. More than ever before, young people are using services such as chat, instant messaging (IM), blogs and social networking sites to communicate with their peers and publish their own content, so they need to develop new skills and awareness in order to remain safe online.

The research evidence

In recent years there has been much research into the use of the internet and digital technologies by children and young people.

The UK Children Go Online (UKCGO)[8] study has found that home access to the internet is growing, that access platforms are diversifying, that children regularly access the internet for activities such as searching and homework, and that most of their online communication is with existing friends.

However, the study also found that children lack key skills in evaluating online content, and many have not received lessons on using the internet. Almost half (46 per cent) of the respondents divulge personal information online, and more than half (57 per cent) of daily and weekly users have come into contact with online pornography. Additionally, one third of daily and weekly users have received unwanted sexual comments (31 per cent) or nasty comments (33 per cent) online or by text message.

[8]See UK Children Go Online website [http://www.children-go-online.net]

Becta recently commissioned the Department of Education and Social Science at the University of Central Lancashire (UCLAN) to conduct an audit[9] to establish the state of e-safety practices in English schools. The findings include the following:

- Breaches of e-safety are most likely to occur among the older pupils in both primary and secondary schools. The most common breach is the viewing of unsuitable online material. However, the research found that where pupils were taught about e-safety, all breaches of e-safety were reduced.
- Breaches are also more likely to occur when pupils are allowed to bring their own personal equipment (such as laptops or portable storage devices) onto school premises. In some cases, such as incidents of bullying via mobile phone, breaches are not only more likely to occur, but also occur with greater frequency when mobile phones are allowed on the premises.
- Teachers' ability to deal with breaches of e-safety varies according to the training and support they receive, the policies and procedures in place in schools and the effectiveness of technical systems.
- Having a designated internet safety co-ordinator in place and having an acceptable use policy (AUP) better equips teachers to deal with breaches of e-safety.

On the basis of these findings, recommendations include that educational establishments take a strategic and integrated approach towards e-safety, with monitoring facilitated by LAs. Educational establishments need to consider alternative ways of managing the use of personal equipment brought onto their premises by pupils, and also to consider issues relating to mobile technologies in e-safety teaching and learning. Targeted directives are required to counter breaches of e-safety within particular pupil groups, while teachers require support that is both tailored to their existing levels of expertise, and that also takes account of the increased capabilities and wider uses of new technologies.

[9] See Becta's Government and partners website [http://partners.becta.org.uk/index.php?section=rh&rid=11302]

Many of these findings and recommendations provide transferable lessons that may help LSCBs to develop effective policy and practice to support all children's services within their remit. Indeed, there are important lessons and best practice to be shared, including how schools have developed effective acceptable use policies (AUPs), provided filtered access to the internet and involved parents. One important starting point for LSCBs and others developing their policies would be to review the way in which schools in their area have developed their duty of care policies for children using the internet, and whether these are appropriate for adoption at a wider local level.

developing a co-ordinated response

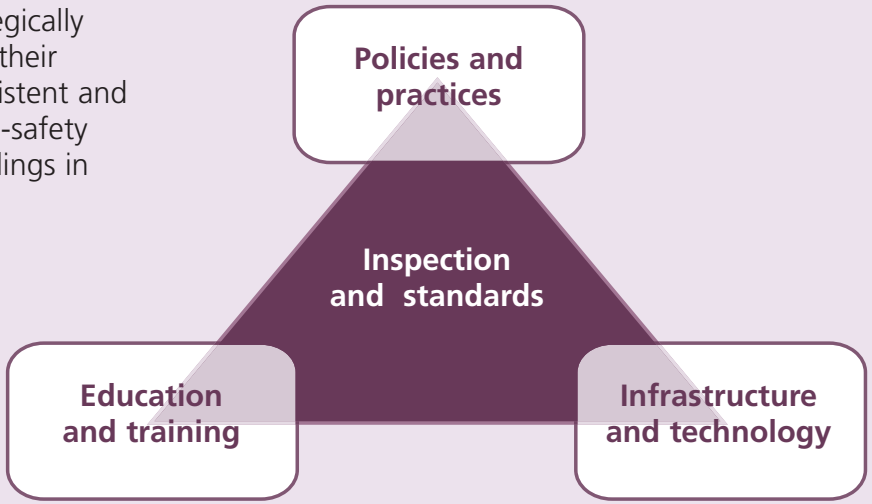
The nature of the UK, and indeed the world, is changing. Learners of the future can look forward to many more opportunities delivered through ICT and personalised learning spaces. Additionally, convergence of technologies means that learning will be less location dependent, and will be able to take place 'anytime, anywhere' at the point of need.

We are already seeing this in the social context, with citizens of all ages grasping the opportunities offered by new technologies that allow them to be always online, connected and contactable. This undoubtedly has many benefits but, as already discussed, it also exposes them to some risks.

Although it will never be possible to remove e-safety risks completely, drawing together an effective package of policies and practices, education and training, and infrastructure and technology – all underpinned by inspection and standards – can lessen the impact of those risks.

Key measures for limiting e-safety risks

LSCBs must work strategically with all services within their remit to achieve a consistent and coherent approach to e-safety under each of the headings in the diagram.



policies and practices

Whatever the context, effective policy is the backbone of good practice, and LSCBs should consider developing comprehensive and coherent e-safety policies for all services within their remit.

Can you answer the following questions?

Co-ordination of activities

Who is responsible for co-ordinating e-safety across the area covered by the LSCB to ensure that best practice is developed, implemented and kept up to date?

We recommend that each LSCB appoint a responsible officer for developing an e-safety agenda across the full range of children's services within its remit. This officer should act as a single point of contact for e-safety issues within the local area and with national agencies such as CEOP (Child Exploitation and Online Protection Centre), ACPO (the Association of Chief Police Officers of England, Wales and Northern Ireland) and Becta.

In individual organisations, who is responsible for co-ordinating the online services provided to and for children and young people?

Each organisation must have a lead person to co-ordinate and focus activities at a local level and to act as a contact point for the LSCB e-safety officer.

Acceptable use policies (AUPs)

Do all services have policies for the acceptable use of ICT by children, young people and staff? Is the application of these policies monitored? Are the AUPs kept up to date in line with changing issues and technologies?

Consider not only the obvious settings such as schools or public libraries, but also places such as youth centres or services where young people might use their own technology.

Are the children and young people that use your services aware of their responsibilities for staying safe online? Are they aware of their responsibilities to others? Do they know who to speak to if they encounter problems online?

Children and young people should be supported in their use of ICT, through education and rules for using the technology safely and clear routes for accessing help and advice.

Is the privacy of children and young people protected when they are online?

If you place photographs of children on your website, for example, you will need to gain permission from the parents or guardian to use those images.

Reporting procedures

What are the procedures for reporting e-safety incidents (regardless of their setting)? How are incidents escalated? What systems are in place for co-operation between agencies in the local area?

Consider, for example, a serious incident in a school where a pupil was found to be distributing images of child abuse on email via the school network. The school would obviously need to report the incident to the police, and to secure and preserve evidence on the school network. However, the incident could also indicate the existence of wider issues, such as sexual abuse within the home or other setting (so normalising behaviours) or peer abuse (so requiring additional support). Is the school clear about the reporting procedure, and do other agencies have the necessary systems in place to support those involved. How would the reporting procedures differ if the e-safety incident occurred in a different setting, for example a public library or hospital school?

All services need to develop and implement clear reporting and disclosure procedures commensurate with the nature of the e-safety incident, and to make staff aware of the issues and co-ordinate responses as necessary.

See Appendix B for a flowchart for reporting e-safety incidents.

Becta recommends…

- That each LSCB appoint a responsible officer for developing an e-safety agenda across the full range of children's services within its remit.

  The e-safety officer should act as a single point of contact on e-safety issues within the local area and with national agencies such as CEOP, ACPO and Becta.

  Appendix A lists the key aspects of this role.
- That the LSCB e-safety officer join the Safetynet mailing list (see the list of resources following).
- That e-safety statements be incorporated into all authority documentation which relates to the safety and wellbeing of children and young people.
- That urgent attention be given to ensuring that each service under the remit of the LSCB meets its requirements under the *Every child matters* programme:
  - Identifying which services provide internet access or allow such access on or from their premises, or other circumstances where the LSCB has an ongoing responsibility for children
  - Developing policies for safeguarding and promoting the welfare of children in the local area (such policies should address training, computer hardware and also internet access for key staff)
  - Ensuring that children's trusts and children's and young people's plans (CYPPs) address the need to safeguard and promote the welfare of children when using ICT (consultation with children and young people should include asking about their online experiences)
  - Developing policies for sharing e-safety information and advice to parents and carers to promote safe use of ICT in the home.

Where services are educational establishments, Becta recommends that policies and practices should be in line with those recommended in *E-safety: Developing whole-school policies to support effective practice* (see the list of resources following). Where services are not educational establishments, these recommendations should be adapted as appropriate to the needs of the service or the setting.

Useful resources

- **Key aspects of the e-safety officer role**

  See Appendix A.

- **Safetynet**

  Safetynet is a Becta-managed mailing list for anyone who wants to discuss and share information to support the development of good practice in e-safety within educational organisations. It aims to provide peer-to-peer support as well as access to the shared knowledge and experience of the community; instant access to colleagues and practitioners, some of who may have similar experiences, difficulties and concerns; and up-to-date e-safety information. You can obtain further information online [**http://lists.becta.org.uk/mailman/listinfo/safetynet**].

- **Examples of good practice**

  There are many examples online of good practice in e-safety and security, such as the materials provided by the South West Grid for Learning (SWGfL) [**http://www.swgfl.org.uk/services/default.asp?page=safety**].

- **E-safety: Developing whole-school policies to support effective practice**

  A major challenge for education practitioners in the 21st century is to prepare a generation of children to become critical and safe users of information and communication technologies. This publication contains 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 recommends practical strategies to follow, drawn up in consultation with the police, should major problems be encountered. You may order or download *E-safety: Developing whole-school policies to support effective practice* from Becta publications [**http://www.becta.org.uk/corporate/publications**].

- **Updated flowchart for dealing with e-safety incidents**

  Appendix B shows a flowchart based on one in *E-safety: Developing whole-school policies to support effective practice*, which we have updated in the light of recent developments in e-safety advice.

- **E-safety materials for parents and carers**

  There are many e-safety resources aimed at parents and carers. The recently updated edition of the Becta publication *Signposts to safety: Teaching e-safety at Key Stages 3 and 4* also includes many pointers to useful resources for parents, as does the companion version for Key Stages 1 and 2.

  LSCBs may also benefit from forming local partnerships, for example with UK online centres, to investigate the possibility of developing e-safety education and training packages specifically for parents and carers.

See also:

Becta website for details of e-safety publications
[**http://www.becta.org.uk/publications**]

UK online centres
[**http://www.ufi.com/ukol**]

infrastructure and technology

As they respond to the challenges of transforming teaching and learning and to the general opportunities offered by new technologies, providers of services to children and young people will face new demands on their technical infrastructures. Increasingly, a strategic response will be necessary.

Can you answer the following questions?

Are there minimum standards of technical e-safety in all settings where children may access ICT?

Technical policies and standards should consider issues such as filtering, the use of accredited ISPs, data security and firewalls. Becta's functional and technical specifications give further information [**http://www.becta.org.uk/industry/techstandards**].

How are these technical standards implemented? Is there scope for local customisation? Is there scope for authority-wide implementation?

All services within the remit of the LSCB should take a strategic approach to managing their technical infrastructures, but must also respond sensitively to local issues, risks or circumstances.

How are technical standards monitored? Are local issues centrally reviewed for evidence of emerging problems or trends?

Monitoring is essential to ensure that systems and procedures are working effectively to protect children and young people. By sharing knowledge and experience of e-safety issues, LSCBs can take a more proactive approach to protecting the children and young people in their care.

Becta recommends…

- That all services within the remit of the LSCB take a strategic approach to managing their technical infrastructures. In support of this recommendation, Becta will continue to promote the use of institutional infrastructure specifications, framework contracts and accredited services as models of good practice. This will also mean institutions are able to enjoy the benefits of being connected to the developing NEN, ensuring they are a part of a wider regional and national approach to e-safety.
- That all services within the remit of the LSCB develop a local implementation plan for filtering and monitoring use of the internet and communications technologies – taking a lead from their LA, regional broadband consortium (RBC) and/or LSCB with regard to both technical solutions and good practice.
- That all services within the remit of the LSCB develop standards of ICT implementation in line with (or based on) Becta's functional and technical specifications (see the list of resources below).

- That all services within the remit of the LSCB consider using a Becta-accredited ISP for their internet connectivity. The main focus of Becta's ISP accreditation has been on accrediting RBC and LA services for schools. LSCBs should consider whether other sectors and services could benefit from the scheme if the criteria are deemed appropriate to the needs of different audiences.
- That the UK Access Management Federation work on school web content authentication and authorisation be adopted to support the development of personalised learning spaces for all learners.

Useful resources

- **Becta's functional and technical specifications**

  The functional specification sets out Becta's vision for institutional infrastructure and considers school ICT from a functional perspective. It gives a detailed breakdown, under four broad headings of the features that learners, educators and administrators should expect from the institution's infrastructure; one of these headings is 'Using ICT to secure data and protect the user'. The technical specification describes how to achieve the functional specification, including wide-ranging detail on safety and security issues. The specification documents are available from Becta's Industry and developers website [**http://www.becta.org.uk/industry/techstandards**].

- **Becta Internet Services Accreditation**

  The service enables schools (and others) to purchase internet services from accredited suppliers that meet and maintain specific standards in content filtering and service performance. For further information on procurement, see the resources section of the Becta Schools website [**http://www.becta.org.uk/schools**].

- **UK Access Management Federation – a strategic approach to school web content authentication and authorisation**

  Becta's work on securely accessing online content for the education sector should be adopted as an integral component in the strategic approach to the future development of ICT in education, skills and children's services. An overview report of Becta's work is available on the UK Access Management Federation site [**http://www.ukfederation.org.uk**].

- **The National Education Network (NEN)**

  It is envisaged that the NEN will provide every teacher and learner with access to a consistent set of resources, services and applications. Baseline standards for safety, security and functionality are being developed to support the NEN [**http://www.becta.org.uk/schools**].

education and training

The responsibility to educate children and young people about the opportunities and risks posed by new technologies belongs to everyone. However, to do this effectively, the educators (whether teachers or other professionals in contact with children and young people) need to be educated themselves.

Can you answer the following questions?

How does the LSCB seek to 'raise awareness about the safe use of the internet' – and other technologies?

As recommended in paragraph 11.62 of *Working together to safeguard children*.

Who co-ordinates key partner activities in the 'development and delivery of training and education programmes with CEOP'?

Also as recommended in paragraph 11.62 of *Working together to safeguard children*.

What standards and protocols for educating and training staff in e-safety issues are in place for all services covered by the remit of the LSCB? How are these training programmes implemented? How are they monitored and evaluated, and how are they kept up to date with the changing online environment?

This should include induction of new staff, plus ongoing support and supervision of existing staff. Staff should be aware of appropriate local, regional and national issues with regard to e-safety, and should be confident in their abilities to escalate an incident as necessary and appropriate.

E-safety and digital literacy skills development should be a continuous process – both for those who are educators (in the formal and informal sense), and also for the children and young people within their care.

Is existing good practice within the authority shared across the LSCB?

Many schools may already be giving extensive e-safety education to their pupils and staff. LSCBs may wish to look at current provision, and assess whether existing knowledge, experience and materials can be shared across other services.

What role is the LSCB playing in ensuring that children and young people outside of mainstream education receive the support and advice they need?

Access to ICT can be particularly beneficial pupils who are unable to attend school regularly, such as those in pupil referral units (PRUs), Traveller children or children attending hospital schools. It can allow them to feel that they remain part of the school environment, and retain some continuity in their work. However, they must also learn how to use the technology safely and appropriately.

What role is the LSCB playing in ensuring that children and young people with special educational needs (SEN) receive appropriate and/or additional support on e-safety issues?

A young person who has a learning difficulty or disability may be especially vulnerable to e-safety risks. They are therefore likely to need additional advice on safe behaviours and what they should never disclose to others online, and they may also need closer supervision. LSCBs must respond to these needs.

What role are non-educational establishments, for example public libraries or youth clubs, playing in educating children and young people in their care and/or using their services?

All services providing ICT access to children and young people have a duty to ensure that they use the technology safely and appropriately.

How will the impact of education and training on children and young people be monitored and evaluated?

Again, e-safety and digital literacy skills development should be a continuous process for children and young people as well as for those who care for them.

What role is the LSCB playing in giving e-safety information and guidance to parents and carers?

Consider what information the LSCB should make available to parents and carers, and how to distribute it. Look for existing opportunities to share information and guidance with parents – for instance via schools, libraries, and Sure Start centres – or for emerging opportunities like the distribution of computer equipment such as Computers for Pupils[10] or other local schemes.

[10]See the Becta website [http://www.becta.org.uk/schools/computersforpupils]

Becta recommends…

- As above, that each LSCB appoint a responsible officer for developing an e-safety agenda across the full range of children's services within its remit.

  The e-safety officer should attend the CEOP and/or NSPCC training schemes on e-safety issues, and cascade this as appropriate to others operating within the area of the LSCB.

  The e-safety officer should also develop links with police agencies and social services to further promote safe internet use.

  On a local level, the e-safety officer should be both proactive in alerting colleagues to new issues and risks, and also reactive in helping with specific incidents as necessary.

  The e-safety officer should retain an overview of education and training programmes at a local level, and should be able to direct colleagues to appropriate resources.

  Appendix A lists the key aspects of the e-safety officer role.

- That e-safety be recognised as an essential aspect of strategic leadership across all services covered by the remit of the LSCB.
- That e-safety and digital literacy skills development be a continuous process both for those who are educators (in the formal and informal sense), and also for the children and young people in their care.
- That LSCBs consider their role in giving e-safety information and guidance to parents and carers.

Useful resources

- **Key aspects of the e-safety officer role**

  See Appendix A.

- **CEOP Training**

  CEOP offer the interactive 'Thinkuknow' programme and training to teachers and educational professionals. This provides knowledge of online issues, necessary child protection information and training on how to deliver the CEOP presentation [**http://www.thinkuknow.co.uk/teachers**].

- **Children and the Net**

  NSPCC is in a position to offer support or training for trainers. Please contact packs@nspcc.org.uk or the Information and Administration Officer, Child Protection Learning Resources, NSPCC Training and Consultancy, 3 Gilmour Close, Beaumont Leys, Leicester LE4 1EZ in the first instance [**http://www.nspcc.org.uk/inform/newsandevents**].

- **University Certificate in Child Safety on the Internet**

  Training for teachers, education and child services professionals to enable them to promote safe and responsible use of internet and mobile technologies and services. Validated by UCLAN [**http://www.internetsafetyzone.co.uk**].

- **Know IT All**

  Interactive resources developed by Childnet International to educate young people, parents and teachers about safe and positive use of the internet [**http://www.childnet-int.org/kia**].

standards and inspection

The inspection of e-safety measures and the monitoring of practices and procedures are essential to ensure that policy is effective, that risks to children and young people are minimised and that, where incidents do occur, all responsible agencies deal with them appropriately.

Under *Every child matters*, children's services are to be inspected to ensure that the five outcomes are being met. Becta urges LSCBs, in association with other inspection bodies, to evaluate local e-safety measures as part of this process.

Can you answer the following questions?

Who is responsible for monitoring e-safety measures across the services covered by the remit of the LSCB? What is the extent of their authority?

As discussed in the policies and practices section, a responsible officer should take the lead in developing an e-safety agenda across the full range of children's services that fall within the remit of the LSCB. This involves monitoring the effectiveness of the e-safety measures in place – including out-of-school and out-of-hours provision.

How is activity monitoring co-ordinated, particularly where several agencies have responsibility in this area?

Here again, it is important for a single responsible officer to take the lead. Co-ordination is essential in order to incorporate recommendations and guidance from all agencies involved in child protection into local e-safety policies and practices.

How is performance measured, and how is progress benchmarked? How is good practice shared? How is poor performance managed? Who drives forward recommendations?

LSCBs may wish to consider developing a set of measures against which to monitor and review e-safety practices. Benchmarking against other LSCBs can help to make sure that everyone follows and shares good practice.

How often is monitoring taking place?

Monitoring must be a frequent and ongoing process to ensure that all services are able to respond to changing issues and risks, and that children and young people continue to be safe and protected.

Who is ultimately responsible? Who inspects the LSCB?

Becta recommends that the evaluation of e-safety measures be included as part of the statutory inspection process.

Becta recommends…

- That evaluation of e-safety measures be included as part of the statutory inspection process.
- That research, evaluation, assessment and monitoring of e-safety provision be ongoing across the LSCB.

Useful resources

- **School self-evaluation framework**
  Ofsted's school self-evaluation framework (SEF) has recently been updated to include reference to the extent to which learners adopt safe and responsible practices in using new technologies, including the internet [**http://www.ofsted.gov.uk**].
- **Local authority self-review framework**
  Becta is developing a new self-review framework to help local authorities to review their own work in supporting schools to improve and raise standards using ICT. Its elements will include leadership and management; learning and teaching; promoting achievement; information management; technology procurement and services; promoting choice, diversity and fair access; and looking at outcomes. The framework will include measures of e-safety maturity and will suggest strategies for further progression.

further information and advice

Becta has produced a number of complementary publications on various aspects of e-safety. Current titles include:

E-safety: Developing whole-school policies to support effective practice

Guidance for schools on developing appropriate policies and procedures to ensure the e-safety of the children and young people in their care

Safeguarding children in a digital world: Developing a strategic approach to e-safety

A strategic overview of e-safety issues for policy makers, outlining a model for a co-ordinated approach by all of the key stakeholders in a child's education

Signposts to safety: Teaching e-safety at Key Stages 1 and 2

Signposts to a selection of resources to help teachers of Key Stages 1 and 2 teach e-safety messages in the classroom, along with appropriate curriculum links

Signposts to safety: Teaching e-safety at Key Stages 3 and 4

Similar to the publication above, but for Key Stages 3 and 4.

All titles may be ordered (subject to availability) or downloaded as PDF documents from Becta publications [**http://www.becta.org.uk/publications**].

You can also find further information on the Becta Schools E-safety website [**http://www.becta.org.uk/schools/esafety**].

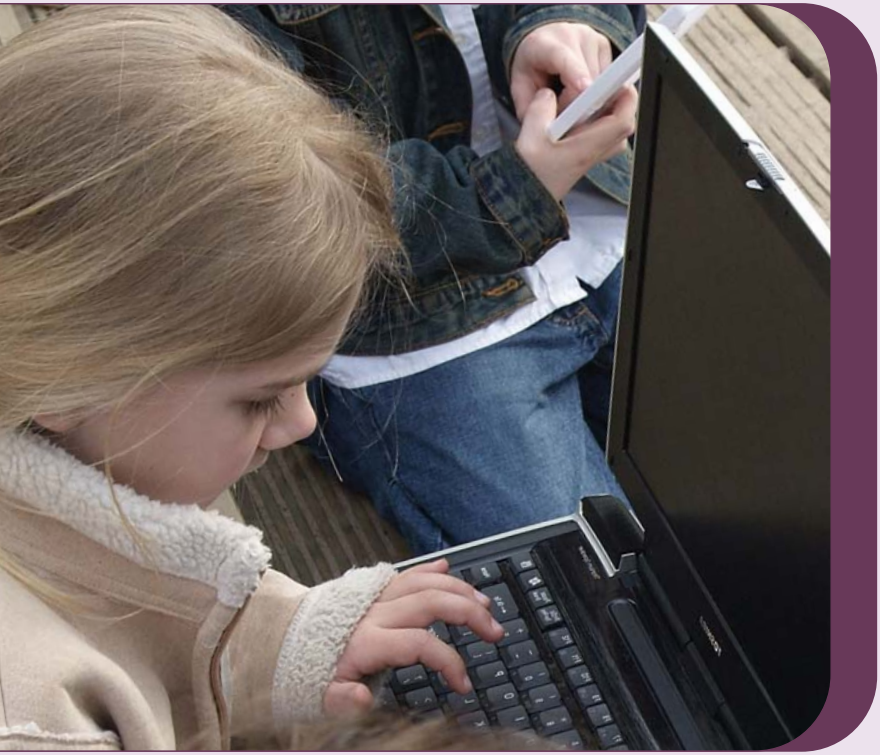
Additional support is available from the Safeguarding Team at Becta and from the Safetynet online mailing list [**http://lists.becta.org.uk/mailman/listinfo/safetynet**].

appendix A

key aspects of the e-safety officer role

The following descriptors outline the key aspects of the e-safety officer role. We recommend LSCBs to consider them when developing a job profile or description.

- Acting as a single point of contact for e-safety issues within the local area
- Supporting the national e-safety strategy



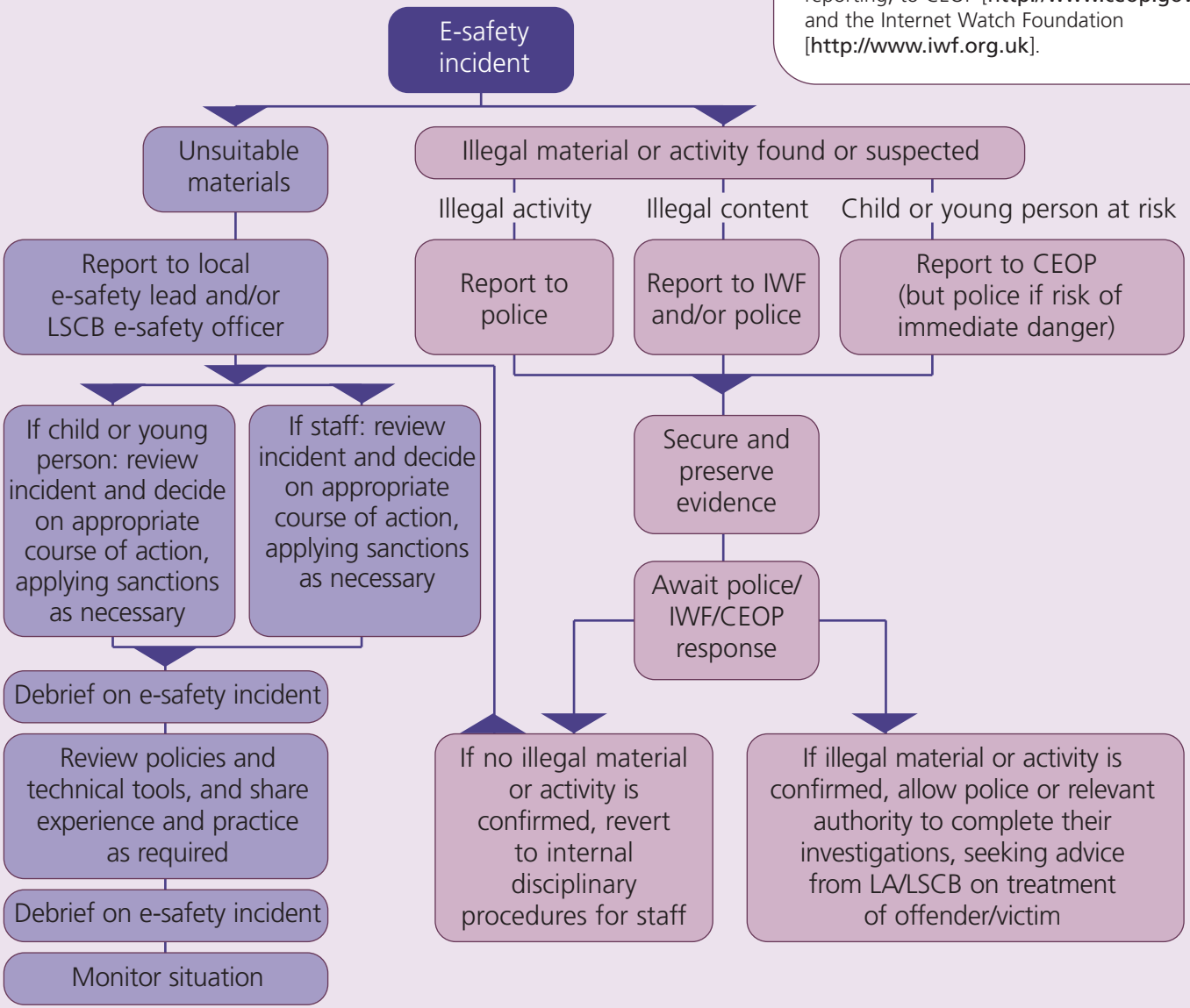
- Liaising with national and international organisations (such as CEOP, Becta and the Virtual Global Taskforce)
- Creating and managing a multi-agency e-safety board
- Creating a dynamic and immediate online communications channel that communicates and raises awareness of e-safety issues with schools and LA stakeholders (using tools such as blogs and other online resources as appropriate)
- Developing collaborative multi-agency policies and approaches for online safety
- Being aware of potential risks from new and emerging technologies and, if appropriate, communicating these to stakeholders with recommendations
- Providing training and supporting resources to schools
- Providing an information and contact point on e-safety issues
- Handling press enquiries and requests for information.

Becta acknowledges the assistance of Kent County Council in supplying this information.

appendix B

flowchart for responding to e-safety incidents

Note: this flowchart originally appeared as 'Flowchart for responding to internet safety incidents in school' in the Becta publication *E-safety: Developing whole-school policies to support effective practice*. We have revised and updated it to include additional lines of reporting, to CEOP [**http://www.ceop.gov.uk**] and the Internet Watch Foundation [**http://www.iwf.org.uk**].



Becta would like to thank the members of the Safe Use of ICT in Education (SUICT) Advisory Group for their support in the writing of this publication.

Advisory Group membership

AoC NILTA [**http://www.aocnilta.co.uk**]

Association of Directors of Children's Services (ADCS)

Association of School and College Leaders [**http://www.ascl.org.uk**]

Association for Information Technology in Teacher Education [**http://www.itte.org.uk**]

BESA (British Educational Suppliers Association)[**http://www.besanet.org.uk**]

Cabinet Office [**http://www.cabinetoffice.gov.uk**]

Child Exploitation and Online Protection Centre (CEOP) [**http://www.ceop.gov.uk**]

Childnet International [**http://www.childnet-int.org**]

Children's Charities' Coalition for Internet Safety (CHIS)

Cyberspace Research Unit (CRU), University of Central Lancashire (UCLAN) [**http://www.uclan.ac.uk/host/cru**]

DfES [**http://www.dfes.gov.uk**]

Home Office [**http://www.homeoffice.gov.uk**]

Internet Watch Foundation [**http://www.iwf.org.uk**]

ISPA UK (Internet Services Providers' Association) [**http://www.ispa.org.uk**]

Learning and Skills Council [**http://www.lsc.gov.uk**]

Naace [**http://www.naace.org**]

National Confederation of Parent Teacher Associations (NCPTA) [**http://www.ncpta.org.uk**]

NSPCC [**http://www.nspcc.org.uk**]

Ofcom [**http://www.ofcom.org.uk**]

Ofsted [**http://www.ofsted.gov.uk**]

QCA (Qualifications and Curriculum Authority) [**http://www.qca.org.uk**]

Regional Broadband Consortia [**http://www.ja.net/community**]

TDA (Training and Development Agency for Schools) [**http://www.tda.gov.uk**]

UKERNA (United Kingdom Education and Research Networking Association) [**http://www.ukerna.ac.uk**]


Fire alarm
WE ARE THE CONSONANTS
How Do You Feel Tod
Happy
Sad
Sorry
Proud
Shy

Millburn Hill Road
Science Park
Coventry CV4 7JJ
Tel: 024 7641 6994
Fax: 024 7641 1418
Email: becta@becta.org.uk
URL: http://www.becta.org.uk

1/DD06-07/100/MP/1k