Safeguarding children in a digital world

Developing a strategic approach to e-safety

Becta
ICT Advice





This publication is intended to provide 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. The guidance in this publication refers to policies and documentation related to England. However the principles discussed have resonance across the UK and beyond.

It is not intended to cover the specifics of e-safety issues or technologies, which you can find in previous Becta publications such as the *Internet proficiency scheme*[1] for Key Stage 2 pupils, *Signposts to safety*[2] for teaching internet safety at Key Stages 3 and 4, and *E-safety: Developing a whole-school approach to internet safety*[3].

Where we use the terms 'e-safety' and 'online', we refer to all fixed and mobile technologies which children and young people might 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.

[1] See Becta publications [http://www.becta.org.uk/publications/] for further information and order details

[2] See Becta publications [http://www.becta.org.uk/publications/] for further information and order details

[3] See Becta publications [http://www.becta.org.uk/publications/] for further information and order details

Contents





Executive summary and recommendations

Becta would like to see a considered approach to developing an e-safety strategy, drawing together policies and practices, education and training, and infrastructure and technology – all underpinned by inspection and standards. To do this will need co-operation from all those involved in the education and wellbeing of children and young people, whether working at national, regional or local level, or in other stakeholder contexts such as industry and the voluntary sector. This strategy makes a number of recommendations about how to achieve this.

Although we have written this document primarily with education in mind, it is likely that many of the issues raised will have an impact on all organisations that deal with the support and wellbeing of children, young people and indeed lifelong learners of all ages, and we hope that some of the recommendations we make will be transferable to other contexts.

Our recommendations on e-safety policies and practices

- That Becta support Government in determining the right structure to drive forward a programme to implement the digital strategy.[4]
- That Becta continue to support the establishment of the Child Exploitation and Online Protection (CEOP) Centre, enhancing its effectiveness specifically in the area of harm reduction and development of e-learning resources for children, teachers and other key stakeholders.
- That Becta work with the DfES to ensure that e-safety guidance is incorporated in its guidance on child protection issues.

[4] See Connecting the UK: the digital strategy [http://www.strategy.gov.uk/downloads/work_areas/digital_strategy/report/index.htm] hereafter referred to as the digital strategy

- That directors of children's services for each local authority nominate a single point of contact within the authority to lead on e-safety work. Urgent attention should be given to ensure that every local authority meets its requirements under the Every child matters programme, which should include the following:
    - Identifying which children's services provide internet access or allow such access on or from their premises, or other circumstances where it has an ongoing responsibility for children
    - Developing policies for safeguarding and promoting the welfare of children in an ICT environment in the local area. Such policies should address training and computer hardware requirements, and also internet access for key staff
    - Ensuring that children's trusts and children and young people's plans (CYPPs) address the need to safeguard and promote the welfare of children in an ICT environment. Consultation with children and young people should include asking about their online experiences.
- That each educational establishment appoint an e-safety and security co-ordinator responsible for the development and implementation of local systems and procedures for ensuring e-safety, who will link with their peers to form a national e-safety network.
- That Becta support the continued development of industry codes of practice for tools and services for promoting e-safety in schools and colleges, at home, and in other markets aimed at children and young people.
- That Becta seek to develop a framework for involvement with partners in the area of ongoing research and evaluation on e-safety issues, and in the benchmarking of best practice.
- That Becta encourage and share best practice in this area with education authorities worldwide.

Our recommendations on e-safety education and training

- That Becta seek to work with the QCA to make explicit the position of e-safety in the National Curriculum in the short to medium term, and contribute to the continuing debate.
- That e-safety education and digital literacy skills development should continue throughout the learner's lifetime.
- That Becta seek to work closely with organisations that are encouraging young people to create their own e-safety learning resources. Resources should be relevant, engaging and creative for this age group, involving children and young people where appropriate in the design, creation and evaluation of resources for their peers.
- That e-safety training be embedded in all initial teacher training (ITT) and continuing professional development (CPD) courses for teachers, and in relevant training for all educational support staff.
- That e-safety be specifically referenced in the Training and Development Agency (TDA) Standards for award of qualified teacher status (QTS) documentation.[5]
- That e-safety be recognised as an essential aspect of strategic leadership.
- That each educational establishment embed e-safety issues within the wider TDA CPD framework.
- The development of volunteer schemes to match the expertise of industry to the needs of parents and communities as part of the extended schools agenda where learning could take place within the school or equally within another external organisation.

[5] See Training and Development Agency website [http://www.tda.gov.uk/partners/ittstandards/standards.aspx]





- That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too.
- That industry rise to the challenge of developing good quality e-safety teaching resources in response to changing requirements of the curriculum, and the continuing needs of lifelong learners.

Our recommendations on e-safety infrastructure and technology

- That local authorities and regional broadband consortia (RBCs) 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.
- That individual schools and colleges develop a local implementation plan for filtering and monitoring use of the internet and communications technologies, and responding to violations (taking a lead from their local authority or RBC as appropriate with regard to both technical solutions and good practice).
- Recognising that it is a viable solution for the education sector, the adoption of Shibboleth for online resource authentication and authorisation, and to support the development of personalised online learning spaces for all learners.

Our recommendations on e-safety inspection, standards and ongoing assessment

- That evaluation of e-safety measures be included as part of the inspection process.
- That QCA review the position of e-safety awareness and digital literacy within its curriculum, assessment and regulatory frameworks.
- That awarding bodies recognise e-safety issues and take steps to ensure that the examination process itself is safe, as assessment becomes increasingly dependent on ICT.
- That research, evaluation and assessment into e-safety provision be on-going and appropriately funded and that Becta play a strategic role in co-ordinating and reviewing this activity.





Introduction

Speaking at an internet safety seminar back in 2001, Michael Wills[6], then Minister for Learning and Technology, said:

'The internet and email are powerful tools to open up new opportunities for people of all ages. The Government wants everyone to have access to the wealth of cultural, scientific and intellectual material to be found on the internet. But we are equally determined to ensure that pupils are protected from unsuitable material and that they can access appropriate material safely.'

This situation has clearly not changed, and with the launch in 2005 of the Government's e-strategy, Harnessing technology: Transforming learning and children's services[7], the prospects for children and learners of all ages to embrace the new opportunities offered by ICT are set to grow.

What we must ensure, however, is that the e-safety aspects are not left to chance. Children and indeed learners of all ages need to develop digital literacy skills that help them to become safe and responsible users of new technologies, and allow them to be discriminating users of both the content they discover and the contacts they make when online.

Since 1998 Becta, in conjunction with the Department for Education and Skills (DfES), has been providing advice and guidance to schools and local education authorities (LEAs) on all aspects of e-safety through the Superhighway Safety website[8].

Highlighting the key safety issues, the Superhighway Safety website has continued to provide practical information and advice for schools on how to use the technologies safely, and has been constantly updated to reflect the new technologies and issues which face education today. Over the years, the website has been supported by a number of publications

aimed at practitioners, including the publications listed on the inside cover of this booklet.

Recognising that e-safety issues are not just the responsibility of practitioners, Becta has also been keen to promote the role of infrastructure and policy in e-safety.

We set up the Becta Accreditation of Internet Services to Education scheme[9] on behalf of the DfES as part of the wider strategy to address internet safety in education, and to complement the information provided via the Superhighway Safety website. The scheme enables schools to purchase services from accredited suppliers that meet and maintain specific standards in content filtering and service performance. All accredited suppliers have gone through a comprehensive testing process and Becta has used standard criteria to evaluate the services of each provider to ensure that they can offer the core minimum requirements. The accreditation not only includes commercial internet service providers (ISPs), but is also open to the many public bodies, such as LEAs and RBCs, that provide internet services to education.

Policy issues have been promoted in various ways. A Becta-hosted seminar at the Education Show in March 2001 sought to raise awareness in this area, explaining new policy and outlining how the Government was tackling the issues. The invited audience included representatives from government departments, LEAs, industry, practitioners and children's charities.

Continuing this work, Becta has also been a key contributor to the DfES-chaired Safe Use of the Internet Steering Group, which was convened in late 2001 to advise the Secretary of State for Education and Employment on internet safety issues. Becta has also been an active member of the Home Office Taskforce on Child Protection on the Internet, and has contributed to many internet safety initiatives in the UK and beyond.

There is now strong UK leadership on the issue of safe use of the internet and online technologies, and this is recognised worldwide. Much is being done throughout the UK to protect children and young people using the internet and communications technologies, but some of this activity is carried out in isolation, without reference to work under way elsewhere.

Becta has therefore convened the Safe Use of ICT in Education Steering Group to revitalise the debate on how we can ensure a strategic approach to e-safety by all those involved in the education and wellbeing of children and young people. It is from the work of this group that this publication stems.

[6] See Becta press release: Becta News at the Education Show 2001: Internet safety seminar [http://www.becta.org.uk/corporate/press_out.cfm?id=1550]

[7] See Harnessing Technology: Transforming learning and children's services [http://www.dfes.gov.uk/publications/e-strategy]

[8] Materials from the original Superhighway Safety website are now hosted and maintained on the Becta Schools website [http://becta.org.uk/schools/esafety]

[9] See Becta Accreditation of Internet Services to Education Scheme [http://ispsafety.ngfl.gov.uk]





E-safety and digital literacy – an overview of the issues

'Our plans for boosting performance and standards across education are far reaching and radical. We aim to put learners, young people – and their parents – in the driving seat, shaping the opportunities open to all learners to fit around their particular needs and preferences.'

Ruth Kelly
Secretary of State for Education and Skills
Taken from the foreword to
Harnessing technology: Transforming learning and children's services

Transforming learning

Harnessing technology sets out the Government's plans for taking a strategic approach to the future development of ICT in education, skills and children's service. It includes four overarching objectives:

- To transform teaching and learning, and help to improve outcomes for children and young people, through shared ideas, more exciting lessons and online help for professionals
- To engage 'hard to reach' learners, with special needs support, more motivating ways of learning and more choice about how and where to learn
- To build an open accessible system, with more information and services online for parents and carers, children, young people, adult learners and employers; and more cross-organisation collaboration to improve personalised support and choice
- To achieve greater efficiency and effectiveness, with online research, access to shared ideas and lesson plans, improved systems and processes in children's services, shared procurement and easier administration.

These objectives will be achieved through six priorities:

Priority 1: An integrated online information service for all citizens

Building an integrated service of information, advice and guidance collected from all relevant organisations within education and children's services

Priority 2: Integrated online personal support for children and learners

Aiming for online personalised support for learners, parents and practitioners, giving secure access to personal records, online resources, tracking and assessment that works across all sectors, communities and relevant public and private organisations

Priority 3: A collaborative approach to personalised learning activities

Transforming how people learn by harnessing the full potential of new technology across all subjects and skills development, and embedding assessment more appropriately within learning and teaching

Priority 4: A good-quality ICT training and support package for practitioners

Defining a minimum level of ICT competence for teachers and other practitioners, promoting new ways of working and of supporting parents, learners and employees, enabling all staff to become effective ICT users and innovators

Priority 5: A leadership and development package for organisational capability in ICT

Helping leaders to assess how well their organisation uses ICT, and to adopt or share good practice, work with others, and plan their approach to ICT as part of their future strategy

Priority 6: A common digital infrastructure to support transformation and reform

Developing high-speed access to robust and sustainable e-systems for all organisations across the sectors based on a common systems framework and technical standards for the software and systems needed to support the strategy, and providing best-value ICT procurement frameworks that are available to all organisations

Each of these priorities will have a significant impact on how learners and teachers use ICT, and will bring with it new challenges to ensure that the e-learning environment is both safe and secure, and that users – children and parents alike – know how to use online resources safely and appropriately.

For example, priority 1 will allow learning to take place where and when the learner wants to learn, at a pace and in a style that best suits their needs. Learning will no longer be confined to the classroom and school hours, where access can be largely controlled and monitored, so safety and security will become crucial.

Under priority 2 there will be a need to ensure that personalised learning spaces are safe and secure, and that authentication systems are both reliable and free from misuse.

Priority 3 will require a review of the curriculum and qualifications to reflect the impact of technology on learning, and e-safety education and digital literacy should form part of the assessment process.

Under priority 4 there will be a need for teachers and other practitioners to have a minimum level of awareness and competence in e-safety issues, in addition to general ICT competence, if they are to support those in their care in becoming safe and discriminating users of new technologies.

Priority 5 will bring with it a requirement for leaders to take strategic responsibility for ensuring e-safety across their services and organisations.

Priority 6 will require that that all organisations involved in the care and education of children and young people ensure that their technological systems and infrastructures can offer the best possible protection in the form of filtering, blocking and similar systems, working to common technical standards and specifications for interoperability, accessibility, quality of service and safety.

Before we look at the solutions for ensuring e-safety, however, it is perhaps useful to revisit some of the issues.





The issues and risks

ICT can offer many positive educational and social benefits to young people, but unfortunately there are risks, too. As in any other area of life, children and young people are vulnerable and may expose themselves to danger – knowingly or unknowingly – when using the internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

One of the key risks of using the internet, email or chat services, is that young people may be exposed to inappropriate material. This may be material that is pornographic, hateful or violent in nature; that encourages activities that are dangerous or illegal; or that is just age-inappropriate or biased. One of the key benefits of the web is that it is open to all, but unfortunately this also means that those with extreme political, racist or sexual views, for example, are able to spread their distorted version of the world.

In the case of pornography and child abuse images, there is no doubt that the internet plays host to a large amount of legal and illegal material. Curiosity about pornography is a normal part of sexual development, but young people may be shocked by some of the material online. It is not known what the long-term effects of exposure to such images may be. Additionally, seeking out some aspects of pornography may be illegal and could result in a criminal conviction.

The threat of physical danger is perhaps the most worrying and extreme risk associated with the use of the internet and other technologies, and is probably the risk most reported by the media. A criminal minority make use of the internet and related services such as chat rooms to make contact with young people. The intention of these individuals is to establish and develop relationships with young people with the sole purpose of persuading them into relationships which they can progress to sexual activity. Paedophiles will often target specific individuals, posing as a young person with similar interests and hobbies in order to establish an online 'friendship'. These relationships may develop over days or weeks, or even months or years, as the paedophile gains the trust and confidence of the young person, perhaps progressing to other forms of contact such as text messaging or phone calls as a prelude to meeting in person. These techniques are often known as 'online enticement', 'grooming' or 'child procurement'.

There is also a risk that while online a young person may inadvertently provide information that can personally identify them or others, or they may arrange to meet people they have met online, so putting at risk their safety or that of their family or friends.

Some young people may get involved in inappropriate, antisocial or illegal behaviour while using digital technologies. Just as in the real world, groups or cliques can form online, and activities that start out as harmless fun, such as voicing an opposing opinion to another member of a chat room, can quickly escalate to something much more serious.

Bullying – whether by internet, mobile phone or any other method – is another aspect of the use of new technologies, which are perceived as providing an anonymous method by which bullies can torment their victims at any time of day or night. While a young person may or may not be in physical danger, they may receive email, chat or text messages that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing.

Some children and young people may become involved in other equally serious activities. Possible risks include involvement in identity theft or participation in hate or cult websites, or in the buying and selling of stolen goods. The ease of access to online gambling, suicide sites, sites selling weapons, hacking sites, and sites providing recipes for making drugs or bombs, are also of great concern. There is some evidence to suggest that young people have become involved in the viewing, possession, making and distribution of indecent and/or child abuse/pornographic images.

In summary, risks associated with using the internet and digital technologies are often categorised as resulting from content, contact, commerce or culture.

Examples of e-safety issues

Content	Contact	Commerce	Culture
• Exposure to age-inappropriate material • Exposure to inaccurate or misleading information • Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance • Exposure to illegal material, such images of child abuse	• Grooming using communication technologies, leading to sexual assault and/or child prostitution	• Exposure of minors to inappropriate commercial advertising • Exposure to online gambling services • Commercial and financial scams	• Bullying via websites, mobile phones or other forms of communication device • Downloading of copyrighted materials e.g. music and films

The research evidence

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

The UK Children Go Online (UKCGO)[10] study offered a rigorous and timely investigation of 9–19-year-olds' use of the internet between 2003 and 2005. The project balanced an assessment of online risks and opportunities in order to contribute to academic debates and developing frameworks for children's and young people's internet use. The study considered factors such as access to the internet, the nature of internet use, inequalities and the digital divide, education and literacy, along with communication and participation. It also considered the risks of undesirable content and online communication, and considered how internet use is regulated in the home.

The study found the following:

- Home access to the internet is growing (75 per cent), and school access is nearly universal (92 per cent)
- Access platforms are diversifying (71 per cent have internet access via a computer, 38 per cent via a mobile phone, 17 per cent via a digital television and eight per cent via a games console)
- Most are daily (41 per cent) or weekly (43 per cent) users, with many children using the internet for searching and homework (90 per cent)
- The internet can encourage participation (for example, 44 per cent of 9–19-year-old weekly users have completed a quiz online, 25 per cent have sent an email or text message to a website, and 22 per cent have voted for something online), and involvement in civic issues (54 per cent of 12–19-year-olds who use the internet at least weekly have used sites concerned with political or civic issues)
- The internet can also provide a source of advice (25 per cent of 12–19-year-old daily and weekly users say they go online to get advice)
- Contrary to public perception, there is little reported interest in contacting strangers online, and most online communication is with existing friends – and generally by mobile phone in preference to emailing or instant messaging.

However, the study also found the following:

- Children lack key skills in evaluating online content (38 per cent of pupils aged between 9 and 19 trust most of the information on the internet, and only 33 per cent of daily and weekly users have been taught how to judge the reliability of online information)

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





- Many have not received lessons (30 per cent of pupils aged 9–19-year-olds report having received no lessons) on using the internet
- Children divulge personal information online (46 per cent)
- More than half (57 per cent) of 9–19-year-old daily and weekly users have come into contact with online pornography
- Most pornography is viewed unintentionally (38 per cent have seen a pornographic pop-up advert while doing something else, and 36 per cent have accidentally found themselves viewing a pornographic website while looking for something else).

The authors of the study concluded that:

'…the risks do not merit a moral panic, and nor do they warrant seriously restricting children's internet use because this would deny them the many benefits of the internet. Indeed, there are real costs to lacking internet access or sufficient skills to use it.

'However, the risks are nonetheless widespread, they are experienced by many children as worrying or problematic, and they do warrant serious intervention by Government, educators, industry and parents.'

Among their many policy recommendations – aimed at policy makers, internet service providers (ISPs), teachers, parents and children – were those of improving levels of internet literacy, developing critical evaluation skills, continuing efforts to prevent exposure to undesirable content and maintaining internet safety awareness.

There is a clear need, therefore, to educate children and young people about the issues and risks. While some parents and carers will have an awareness of the issues, others will not, so it is unrealistic to place this responsibility on them. Educational establishments thus have a major responsibility to educate their students as part of the wider duty of care, teaching them the appropriate behaviours and critical thinking skills to remain both safe and legal online, wherever their learners use technology.

However, as the UKCGO evidence shows, many children are lacking in basic education and awareness when it comes to e-safety issues, and it appears that schools are at very different stages in their approach to e-safety. This is further supported by recent Becta research. In 2005 Becta commissioned the Department of Education and Social Science at the University of Central Lancashire (UCLAN) to conduct an audit of e-safety practices in English schools. The aim of the research was to establish the current level and range of activity in schools to ensure the safe and effective use of digital and communication technologies.

The research consisted of two phases. In the first phase a total of 444 schools – 303 primary and 123 secondary, plus a small number of pupil referral units (PRUs), special schools and FE providers – completed a postal survey to examine three key areas: school policies; technical infrastructures in place; and pedagogical provision and approaches to teaching pupils about e-safety. The second phase involved one-to-one telephone interviews with 61 teachers in order to explore these issues in greater depth. The research also included a sample of LEAs and RBCs (25 and 5, respectively) to explore the forms of provision and support they offer to schools across the country.

The audit of schools found that while 85 per cent of schools have an acceptable-use policy (AUP) in place, 11 per cent do not. Of those with an AUP, there are low levels of involvement in the creation of the policy beyond the headteacher and senior management team, and fewer than half of all respondents (47 per cent) reported having a designated internet safety co-ordinator at their school. Additionally, a fairly low number of schools (34 per cent) have developed their AUP in conjunction with, or in relation to, other school policies. There is therefore a concern that schools are not yet in a position to take a strategic approach to e-safety issues.

While AUPs cover well such issues as use of the internet and email (98.5 per cent and 95 per cent respectively), they are less likely to cover issues regarding personal technologies or technologies that are not permitted in schools, such as mobile phones, despite pupils' heavy recreational use of these. This is also reflected in the degree to which schools feel their pupils need advice about certain e-safety issues: schools reported that they felt pupils needed to be taught more about plagiarism (38 per cent), viewing of unsuitable material (33 per cent) and bullying via chat rooms (29 per cent), but felt that guidance on inappropriate use of mobile phones (21 per cent) and bullying via this technology (25 per cent) was less necessary. This suggests that children and young people may seriously lack guidance about the risks and on how to use technologies safely when not in the fairly protected confines of their school or college.

The audit of LEAs and RBCs resulted in a fairly low response rate (which in itself may indicate a lack of strategic approach in this area), but nevertheless gives some useful insights.

A fairly high proportion of LEAs and RBCs provide support for schools regarding technical issues (88 per cent and 80 per cent respectively), along with support on e-safety policies and procedures (100 per cent and 80 per cent respectively). All respondents reported that they distribute sample AUPs to schools. However, (and this reflects the schools findings), the information from LEAs and RBCs tends to focus on the longer-established elements of the internet typically encountered within the school setting, as opposed to mobile technologies.

Just 24 per cent of LEA respondents and 40 per cent of RBC respondents had received training on e-safety issues, yet 57 per cent of LEAs and 67 per cent of RBCs said they had provided training for teachers on e-safety issues. Encouragingly, though, 62 per cent of LEAs and 67 per cent of RBCs provide schools with access to e-safety teaching materials or resources for pupils.

In terms of their changing roles with regard to child protection, of the 25 LEAs and 5 RBCs that responded, only one LEA and no RBCs said they had considered how issues relating to online safety will be incorporated into arrangements to safeguard the welfare of children under section 11 of the Children Act 2004. Meanwhile three LEAs and one RBC had not considered this, and 19 LEAs and three RBCs were still unclear how to proceed.

The full findings of the E-safety in English schools audit are published as a research report on the Becta website[11].

The challenge, therefore, is to take a strategic approach to e-safety: one which protects and educates children and young people through effective solutions that combine both safe practices and safe systems.

[11] See Becta research website [http://www.becta.org.uk/research/reports/esafetyaudit]





The wider strategic context for e-safety

There is increasingly a wider strategic context within which e-safety falls, mainly embedded within child protection strategies.

E-safety – the strategic context

- The Children Act 2004
- Every child matters: Change for children
- Safeguarding children in education
- Connecting the UK: The digital strategy
- Harnessing technology: Transforming learning and children's services

Child protection strategies

In the wake of reports from the Victoria Climbié Inquiry[12] and the Bichard Inquiry[13], arrangements to safeguard and promote the protection of children and young people are high on the agenda of every local authority. There are several key strategies within this area.

The Children Act 2004[14] provides a legislative framework for wider strategies for improving children's lives. The overall aim is to encourage integrated planning, commissioning and delivery of services to children, and to improve multidisciplinary working. The act provides the legal underpinning to Every child matters: Change for children[15].

[12] See the Victoria Climbié Inquiry [http://www.victoria-climbie-inquiry.org.uk]

[13] See the Bichard Inquiry [http://www.bichardinquiry.org.uk]

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

[15] See Every child matters: Change for children [http://www.everychildmatters.gov.uk]

In Every child matters, the Government sets out its aims for every child and young person (from birth to age 19) to have the support they need to achieve five key outcomes:

- Be healthy
- Stay safe
- Enjoy and achieve
- Make a positive contribution
- Achieve economic well being.

As part of the implementation process, children's services will be inspected[16] to ensure that each of the five outcomes are being met. Such inspection will encompass not only education, but areas such as social services functions for children and young people, and play and leisure services.

The 'stay safe' outcome, for example, includes aims that children and young people are:

- 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.

Although undoubtedly these aims were written with the 'real world' in mind, many equally apply to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used 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 can sometimes lead to their involvement in crime and anti-social behaviour.

To ignore e-safety issues when implementing the requirements of Every child matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable.

Safeguarding children in education[17] outlines a shared objective for all those working in education services to help keep children and young people safe by contributing to the following objectives:

- To provide a safe environment for children and young people to learn in education settings
- To identify children and young people who are suffering or likely to suffer harm, and to take appropriate action with the aim of making sure they are kept safe both at home and at school.

The first objective places a clear responsibility on educational establishments to provide a safe e-learning environment through a combination of technical infrastructures and effective policies and practices.

When we consider the second objective also, we can see a clear responsibility to educate children and young people in how they can remain safe in the virtual world, regardless of whether they are likely to encounter the risks at school, at home or in any other setting.

[16] See Every child matters: The framework for inspection of children's services [http://www.ofsted.gov.uk/everychildconsultation]

[17] See Teachernet [http://www.teachernet.gov.uk/wholeschool/familyandcommunity/childprotection]





Digital strategies

The Government has a strong commitment to using new technologies as a means of ensuring that the UK can remain globally competitive, but it has also committed itself to enabling the whole of our society to experience the benefits of the internet and ICT.

Issues relating to the digital divide are addressed in Connecting the UK: the digital strategy[18]. In that report, the Government sets out its plans to make the UK a world leader in digital excellence, minimise social exclusion and close the digital divide, and protect consumers from the dangers of the 'darker side' of the digital world.

The report sets out eight key actions:

1 Transforming learning with ICT

2 Setting up a 'digital challenge' for local authorities to achieve both excellence and equity in ICT

3 Making the UK the safest place to use the internet

4 Promoting the creation of innovative broadband content

5 Setting out a strategy for transforming delivery of key public services

6 Ofcom to set out a regulatory strategy

7 Improving accessibility to technology for the digitally excluded and ease of use for the disabled

8 Reviewing the digital divide.

We can clearly see the importance of e-safety within the overall strategy, particularly under Action 3.

The digital strategy recognises a need to ensure that everyone, particularly parents and children, are confident in how to manage effectively the day-to-day risks of using the internet. To achieve this, the strategy recommends a number of new measures, including the development of a multi-agency national internet safety centre, improvement of online identification and identity management, and better use of tools – such as parental controls, firewalls and web-blocking technology – for managing digital content.

Recognising the role of education, and building on Action 1 of the digital strategy, is the e-strategy, Harnessing technology: Transforming learning and children's services, as already discussed.

[18] See the digital strategy [http://www.strategy.gov.uk/work_areas/digital_strategy]

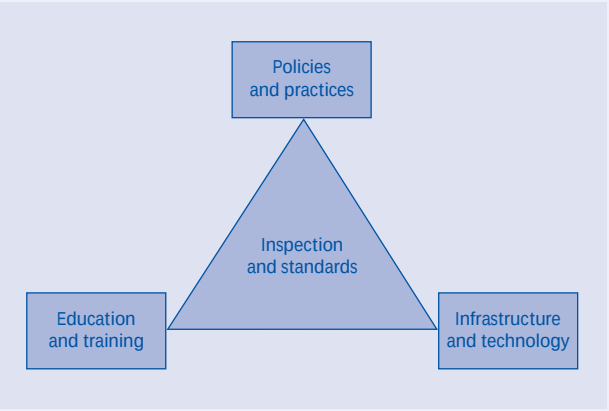




Becta's view – a co-ordinated approach

The shape of education is changing in the UK, and 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.

However, there are some risks to the safety and wellbeing of learners when using online content, services and digital technologies. Although it will never be possible to remove these 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 their impact.



Limiting e-safety risks: Key measures

Becta would like to see a considered approach to developing an e-safety strategy, drawing together each of these elements. To achieve this needs co-operation from all those involved in the provision of services to children and young people, whether working at national, regional or local level, or in other stakeholder contexts such as industry and the voluntary sector.

It makes sense for e-safety education to be firmly embedded in frontline service provision – the practitioners who are in daily contact with children and young people, and who will often be the first point of contact should issues arise. To do this, however, practitioners need to feel confident that they are supported, whether through continuing professional development to raise their awareness of the issues and risks, clear policies and practices to support them in their daily work, a robust technical infrastructure, or being allowed time in an already crowded curriculum to educate the young people in their care.

To support individual educational establishments in this process, there needs to be a strong commitment to e-safety at local authority level. Under Every child matters and the creation of new children's services, all local authorities have a clear responsibility to ensure that children and young people stay safe. Directors of children's services (DCS) must understand that e-safety is part of this remit. They must work strategically with all educational establishments to achieve a consistent and coherent approach to e-safety, putting in place framework contracts and accredited services wherever possible, and setting up effective monitoring and inspection systems to meet the e-safety challenges.

We have already spoken about the requirement to embed teaching of e-safety within the curriculum, but at present, schools are not clear about any statutory requirements. There should be a mandatory requirement for all children and young people to receive education on e-safety issues, appropriate to their age and understanding. Additionally e-safety should be taught within other subjects promoting personal health, well-being, and social and moral responsibility, such as PSHE and citizenship, and embedded within other areas of the curriculum, key, or core skills, as appropriate.

As access to ICT and communications technologies continues to grow for all citizens, so new challenges for e-safety will emerge. We must therefore look to industry and the voluntary sector for innovative solutions, whether in the form of new products and services to protect users in the virtual world, codes of practice, or information and support should problems occur.

Although this document is written largely with education in mind, it is likely that many of the issues raised will have an impact on every organisation that deals with the support and wellbeing of children, young people and lifelong learners of all ages. We hope that some of the recommendations we make will be transferable to other contexts.





Policies and practices

There is currently a great deal of activity on e-safety issues by a wide range of organisations such as government departments, non-governmental organisations (NGOs), individual local authorities and RBCs, industry and the voluntary sector. However, some of this activity is carried out in isolation. Each of these individual groups needs to be aware of the full range of issues, but they must also come together, be aware of the overlaps and consider a common framework to move forward.

We therefore make several recommendations on developing effective e-safety policies and practices.

Development of a national e-safety strategy

Becta strongly believes that a co-ordinated approach to developing a national e-safety strategy is necessary.

Clause 63 of the digital strategy states that,

'Under Ministerial ownership, OGC (Office of Government Commerce) and eGU (e-Government Unit) will support DTI (Department of Trade and Industry) in determining the right structure to drive forward a programme to implement the strategy. This will include appropriate representation from government departments, No 10, and other key stakeholders, for example the Broadband Stakeholders Group.'

Becta will support Government to ensure that e-safety and security issues are recognised in the digital strategy at a national level.

Additionally, the protection of children from abuse via ICT needs a multi-agency approach that shares intelligence and resources, develops sensible national policies, and centralises processes. The development of the national Child Exploitation and Online Protection (CEOP) Centre is already in progress, and Becta will offer information, advice and support as necessary for the effective development of this service.

Clarification of the role of children's services

Under Section 11 of the Children Act 2004, local authorities have a duty to ensure that services for children are safe and accessible. One of the key considerations is how to keep children safe while using services, for example, through appropriate supervision by trained staff and by adhering to health and safety regulations.

Under Every child matters, local authorities must take appropriate measures across all services, with clear lines of responsibility and accountability for policy, infrastructure, education and training.

In Becta's view, each children's service should identify a member of staff to co-ordinate e-safety and security issues, and to advise where necessary. This role should have responsibility for all learners in all situations, including those being educated away from typical school environments, or in informal learning settings such as libraries and youth centres. The member of staff should strategically manage and co-ordinate activities across all services, and provide a channel for staff training and continuing professional development on e-safety issues. The CEOP Centre should also be a key partner in this process.

So as to benefit from a wider view, these regional e-safety and security advisers should have a mechanism for communicating effectively with each other at a national level, advising of issues on the ground, and taking back policies and procedures to implement at their respective regional and local levels.

E-safety embedded in DfES advice on child protection

The DfES provides a range of information on child protection issues to schools and local authorities through various channels, including the Teachernet website[19] and the Area Child Protection Committees (ACPC) website[20].

Becta recommends incorporating explicit reference to e-safety issues in all DfES child protection guidance. Becta will support the DfES in ensuring that such guidance is not only current and comprehensive, but also responsive to changing e-safety issues.

Development of organisational policies and procedures

As described in E-safety: Developing a whole-school approach to internet safety, Becta recommends that, as a minimum, schools have an acceptable use policy in place to protect the interests of both pupils and staff (and provide responses to inappropriate use), and that this be at the heart of practice. Becta also recommends identifying a senior manager to co-ordinate all activities relating to e-safety, from policies and practice to technology issues and user education and training.

Additionally, organisations such as the Internet Watch Foundation (IWF) – the UK hotline for reporting illegal content – provide best-practice guides on e-safety issues such as handling potentially illegal images of children[21]. These can be easily adapted for use in educational environments.

[19] See Teachernet website: child protection [http://www.teachernet.gov.uk/wholeschool/familyandcommunity/childprotection]

[20] See Area Child Protection Committees website [http://www.dfes.gov.uk/acpc/]

[21] See Internet Watch Foundation website [http://www.iwf.org.uk/documents/20051111_iwf_best_practice_guide.pdf]





Colleges will also need to ensure that they have adequate measures in place to protect the 14–19 cohort within a predominantly adult environment, while the development of personal learning spaces, as recommended in Harnessing technology, will provide new challenges to ensuring that learners remain safe without infringing their rights to privacy.

Development of industry codes of practice

We must recognise that e-safety is not just an issue for the educational sector. Technology touches us in every part of our daily lives, so there is a responsibility on all to ensure that children and young people are safe, secure and protected. We must therefore look to industry to develop innovative solutions, recommendations and codes of practice to support e-safety issues, aimed at consumers of all ages. This may be in the form of targeted curriculum tools for teaching e-safety, the provision of information and advice on filtering techniques supplied with all PCs, codes of conduct for use of the internet over the range of mobile communication devices, or awareness raising through the mainstream media of new issues and risks in a non-sensationalist way.

Industry support for e-safety issues should be embedded in the digital strategy as discussed above.

International co-ordination and co-operation

One of the benefits of ICT is that it has no geographical boundaries, but this in itself may pose e-safety issues for global communication and learning – particularly if e-safety safeguards and standards in other countries do not match our own.

Becta, with the support of its many partners, will seek to encourage and share best practice in this area with education authorities worldwide, encouraging global practices in education that promote e-safety.

Our recommendations for e-safety policies and practices are therefore as follows:

- That Becta support Government in determining the right structure to drive forward a programme to implement the digital strategy
- That Becta work with the DfES to ensure that e-safety guidance is incorporated in its guidance on child protection issues
- That directors of children's services for each local authority nominate a single point of contact in the authority to lead on e-safety work. Urgent attention should be given to ensure that every local authority meets its requirements under the Every child matters programme, which includes:
    - Identifying which children's services provide internet access, or allow such access on or from their premises, or other circumstances where it has an ongoing responsibility for children
    - Developing policies for safeguarding and promoting the welfare of children in an ICT environment in the local area. Such policies should address training, computer hardware requirements and also internet access for key staff
    - Ensuring that children's trusts and children and young people's plans address the need to safeguard and promote the welfare of children in an ICT environment. Consultation with children and young people should include asking about their online experiences
- That Becta continue to support the establishment of the CEOP Centre, enhancing its effectiveness specifically in the area of harm reduction and development of e-learning resources for children, teachers and other key stakeholders
- The appointment by each local authority of an e-safety and security adviser, who will link with their peers to form a national e-safety network
- That each educational establishment appoint an e-safety and security co-ordinator, responsible for the development and implementation of local systems and procedures for ensuring e-safety
- That Becta support continued development of industry codes of practice for tools and services for promoting e-safety in schools, colleges, at home, and in any markets aimed at children and young people
- That Becta seek to develop a framework for involvement with partners in the area of ongoing research and evaluation on e-safety issues, and in the benchmarking of best practice
- That Becta encourage and share best practice in this area with education authorities worldwide.





The Child Exploitation and Online Protection Centre

The Child Exploitation and Online Protection (CEOP) Centre, which will come into being in April 2006, will work to protect children, families and society from paedophiles and sex offenders; in particular, from those who seek to exploit children sexually online. The centre will achieve this by providing additional support to law enforcement and child protection systems.

Traditionally, law enforcement has concentrated on only one aspect of policing concerning abusive images of children. There is a need to go beyond those who download abusive images of children, by undertaking proactive investigations to identify not only those who perpetrate the abuse of children, but also their victims.

CEOP will be a dynamic partnership between Government, law enforcement, NGOs (including children's charities) and industry, with the common aim of protecting children. Consolidating the existing law enforcement functions that are focused on this type of abuse, the centre will have the following functions:

- To provide a 24/7 single point of contact for law enforcement, industry, NGOs and the public for the reporting of online child abuse in the UK (including the provision of a single point of contact to inform, educate and communicate with victims and potential victims of abuse)
- To receive, assess and disseminate intelligence coming into the UK on online and offline offenders, including paedophiles and other sex offenders
- To establish reporting processes that are efficient, expedient and which minimise delay in responding to risks to children
- To enhance the police's capacity to engage in proactive policing of online child abuse, which by its very nature rarely corresponds with constabulary boundaries
- To support, co-ordinate and assist national and international investigations into online child abuse
- To enhance the police's capacity to identify the victims depicted in the images and provide support for the victims
- To identify and recover criminal assets from those profiting from abuse
- To keep abreast of research, technical developments and risk analysis, so becoming a reference point for the identification of trends and exchange of information
- To deliver, and contribute to the delivery of, comprehensive, specialist and effective educational and training programmes.





Education and training

The digital strategy clearly sets out a challenge to embrace digital technologies for the benefit of all society, and for the UK to lead the way in promoting digital excellence.

An economic digital divide already exists between those that have access to new technologies and those who do not; an educational digital divide exists between those that have access to opportunities to learn and those who have not; and a social digital divide exists between those who embrace these new technologies and those – for moral or cultural reasons – for whom ICT has no place.

A generation of children for whom ICT is a way of life are already passing through the education system. The proliferation of mobile technologies means that the internet is available to them 'anytime, anywhere' via a range of handheld devices, and the convergence of new technologies means that online experiences will become increasingly difficult to regulate.

While there is evidence that the digital divide causes great variations of access for children and young people, it is not uncommon for them to use ICT in a wide and growing range of applications. Some examples include:

- **Education** – research using the internet, word processing, data manipulation, modelling, design and creativity
- **Entertainment and leisure pursuits** – downloading films and music, playing games, communicating with peers and taking, storing, manipulating and retrieving digital images and video
- **Communication** – via voice, email, chat rooms, message boards and forums, instant messaging, text messaging and blogs
- **Personal management** – via online diaries, appointment calendars and address books, alarm clocks and personal reminders
- **Shopping** – where credit cards are available.

To the younger generation, ICT is not a tool for occasional use: it is firmly embedded into their daily life as a way of managing their lifestyle and communicating with their world.

As an educational organisation, Becta must promote e-media education and digital literacy along with the relevant e-safety messages. Children and young people have to learn critical awareness, effective security practices, digital literacy and good online citizenship from an early age. Equally, practitioners must be confident in their abilities to educate children and young people, and should receive continuing professional development to enhance their knowledge and understanding in this area.

We therefore make several recommendations on developing effective e-safety education and training practices.

Improved digital literacy skills for all learners

The Education Act 2002[22], the implementation documentation for the Children Act 2004 and Every child matters: Change for children include a statutory duty for all schools and further education institutions to safeguard and promote the welfare of children.

Staff in these establishments play an important part in safeguarding children and young people from abuse and neglect through early identification of those who may be vulnerable or at risk, and by educating them and improving their resilience through the curriculum. It therefore makes sense, with the increasing use of ICT in the daily life of children and young people, for e-safety education to become an integral element of the curriculum in areas such as ICT, PSHE and citizenship. Additionally, e-media and digital literacy awareness, such as the ability to evaluate critically any materials found online and to recognise issues surrounding copyright and plagiarism, should be reinforced wherever ICT is used in the curriculum.

In the drafting of the ICT functional skills standards, QCA has been working with Becta and other partners to ensure that e-safety is represented in both the definition and the standards on which functional skills qualifications will be based.

It is essential to make e-safety education and policy meet the specific needs of the learner, whether in terms of age appropriateness, or for specific groups of learners such as those with special educational needs or those for whom English is a second or additional language. Children and young people should also be encouraged to become active stakeholders in developing e-safety policies, practices and educational resources. Children and young people can help their peers and their teachers to understand the issues and risks as they perceive them, and we can give them positive opportunities to shape, participate in and evaluate e-safety initiatives. As early adopters of new technologies, children and young people are often the first to use new tools and hence the first to encounter new risks and dangers: the ability to map these experiences, both locally and nationally, can provide useful insights into where we should be directing e-safety resources.

At present, comprehensive good-quality e-safety teaching resources are rare. Apart from the Internet proficiency scheme for Key Stage 2 pupils (produced by Becta in association with the QCA), and recent independent resources for Key Stage 3 produced by non-profit organisations[23], there are few e-safety resources aligned to the National Curriculum. Conversely, as the position of e-safety within the statutory curriculum is not well understood, there is no commercial impetus to create teaching resources on this topic.

[22] See the Education Act 2002 [http://www.opsi.gov.uk/acts/acts2002/20020032.htm]

[23] See 'Know IT All' resources, for example. Produced by Childnet International, these Key Stage 3 resources were distributed to every secondary school in the country in November 2005 [http://www.childnet-int.org/kia].





The QCA project, Futures: meeting the challenge[24], looks at the issues in developing a curriculum for the 21st century. Research has identified five key forces for change:

- Changes in society and the nature of work
- The impact of technology
- New understanding about learning
- The need for greater personalisation and innovation
- The increasing international dimension to life and work.

It seems that the time has come to give greater consideration to e-safety in the curriculum. Becta will therefore seek to work with the QCA to make explicit the position of e-safety in the National Curriculum in the short to medium term, and will contribute to the continuing debate.

It is also important for subject associations to rise to the challenge of how to make e-safety of practical relevance to their subjects, and for examination boards and inspectors to consider how to measure and assess such learning. It is equally important that the emphasis on e-safety issues and digital literacy skills should not cease when a pupil leaves secondary education, but should continue throughout the learner's lifetime.

Improving educational workforce confidence and competence

Harnessing technology: Transforming learning and children's services presents proposals for the QCA, in liaison with the Training and Development Agency for Schools (TDA) and Lifelong Learning UK (LLUK), to develop a national professional development framework for 2007, and this is already under way. It is important that the framework should include an element of e-safety awareness and education. Becta will therefore offer support to these organisations to develop accredited training programmes on e-safety issues for all who work in educational establishments.

Such training should include:

- an overview of the benefits of new and emerging technologies, alongside recognition of the issues and risks
- a focus on teaching digital literacy skills and encouraging children to develop powers of evaluation and judgement
- an understanding of how to identify the behaviours (or changes in behaviour) which could indicate problems relating to use of the internet or digital technologies
- a consideration of the techniques that pupils use to hide inappropriate activity
- an understanding of how to use management information (for example, usage logs) to identify and track problems
- an understanding of the technical issues, such as how to manage filtering and blocking software in the classroom to provide adequate protection without limiting the learning opportunities
- a knowledge of how to appropriately respond to breaches of safety and security measures.

Becta will also work with the National College for School Leadership (NCSL) to ensure that leadership programmes such as the Strategic Leadership of ICT (SLICT) and the National Professional Qualification for Headship (NPQH) include advice and guidance on e-safety and security issues.

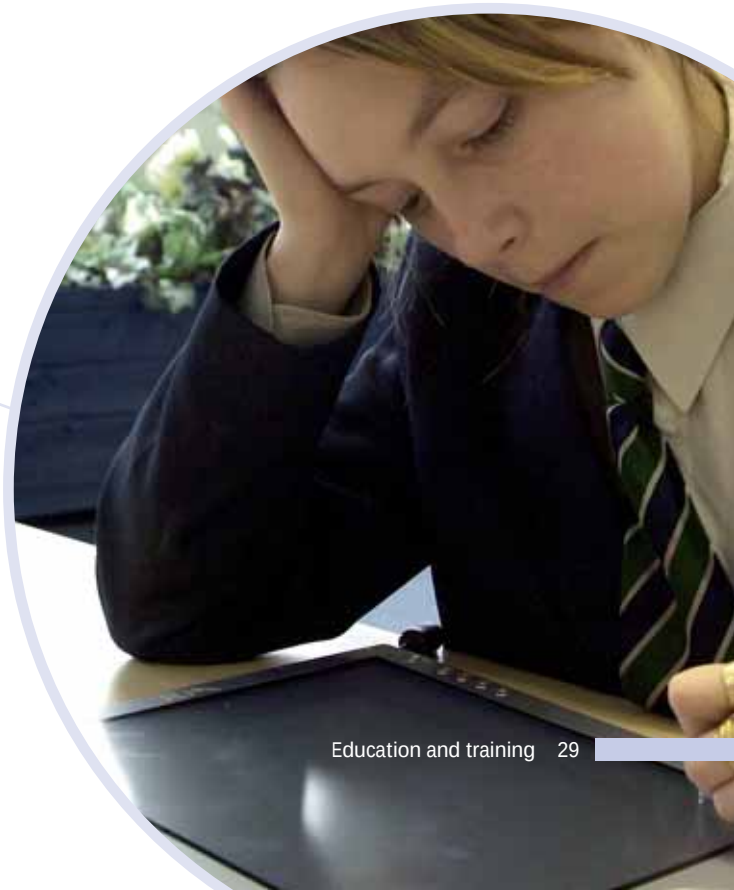
Making best use of wider expertise

In order to establish good practice in e-safety and digital literacy in the education and child protection fields, it is useful to look beyond these sectors at the wider expertise that exists in industry and the voluntary sectors.

[24] See Futures: meeting the challenge [http://www.qca.org.uk/futures]

While recognising that e-safety should be taught by trained teachers, Becta recommends the development of effective volunteer schemes that match the expertise of industry volunteers to the needs of schools, parents and communities. This will not only enable schools to become centres of internet literacy for all, but also help to develop a shared understanding of the issues and risks. Although the extended schools agenda offers an excellent opportunity for doing this, the value of volunteers as a general resource should not be underestimated. Volunteers must be properly recruited, have Criminal Records Bureau (CRB) clearance to work with children and be properly inducted, trained, supervised and supported in their work in schools by an independent organisation[25].

In making this recommendation, Becta wishes to encourage both schools and industry to be proactive in building these relationships, and in helping parents to support their children when online.



[25] The 'Getting to Know IT all' volunteer programme developed by Childnet, Microsoft and the Virtual Global Task Force, in which over 100 volunteers were trained to go into schools, has been evaluated independently by the University of Bristol [http://www.childnet-int.org/kia].





Our recommendations for e-safety education and training are therefore as follows:

- That Becta will seek to work with the QCA to make explicit the position of e-safety in the National Curriculum in the short to medium term, and will contribute to the continuing debate
- That e-safety education and digital literacy skills development continue throughout the learner's lifetime
- That Becta work closely with organisations that are encouraging young people to create their own e-safety learning resources. Resources should be relevant, engaging and creative for this age group, involving children and young people where appropriate, in the design, creation and evaluation of resources for their peers
- That e-safety training be embedded in all initial teacher training and CPD courses for teachers and in relevant training opportunities for all educational support staff
- That e-safety be specifically referenced in the Training and Development Agency (TDA) Standards for award of qualified teacher status (QTS) documentation[26]
- That e-safety be recognised as an essential aspect of strategic leadership
- That each educational establishment embed e-safety issues within the wider CPD framework of the TDA
- The development of volunteer schemes to match the expertise of industry to the needs of parents and communities as part of the extended schools agenda, where learning could take place within the school or equally within another external organisation
- That schools support parents in understanding the issues and risks associated with children's use of digital technologies; that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school; and, recognising the growing trend for home-school links and extended school activities, that schools also provide information and guidance for parents on promoting e-safety messages in the home use of ICT
- That industry rise to the challenge of developing good quality e-safety teaching resources in response to changing requirements of the National Curriculum and the continuing needs of lifelong learners.

[26] See Training and Development Agency website [http://www.tda.gov.uk/partners/ittstandards/standards.aspx]





Infrastructure and technology

There are a number of technological tools that education providers should employ to help safeguard learners and educators as well as the technical infrastructure itself. These include:

- providing a network that protects the user from inappropriate content and ensures data security and integrity
- using a content and email filtering system managed by the LEA or RBC in discussion with relevant institutions (it should also be possible to refine these filters at an institutional level)
- providing safe and secure internet access for every user of the service (managed by the LEA/RBC).

Becta has published a fuller discussion of safety and security issues for educational institutions in the document Functional specification: Institutional infrastructure[27].

Education providers will face new demands on their technological infrastructures as they respond to the challenges of transforming teaching and learning. A strategic response will be increasingly essential.

The National Education Network

Development of the National Education Network (NEN)[28] – providing a coherent system for accessing nationally available educational resources and applications – will also be fundamental in meeting the objectives of the digital strategy.

Becta is compiling a framework of technical and functional standards to underpin the development of the NEN, and will seek to ensure that these standards are maintained and

[27] See Becta Technical policy and standards: Functional specification: Institutional infrastructure [http://www.becta.org.uk/schools/techstandards]

[28] See Becta Building a National Education Network [http://www.becta.org.uk/nen]

implemented appropriately. This includes making a safe online environment available to all educational establishments as a basic entitlement for all learners and teachers.

Services provided via the NEN will need to ensure that they meet minimum requirements, and Becta is therefore working with suppliers to achieve the following objectives:

- A clear definition of the minimum acceptable level of filtering, currently defined in the Becta Accreditation of Internet Services to Education scheme[29]
- Thorough on-site testing and quality assurance of services
- Agreement of action plans where services do not meet requirements
- Monitoring of action plans until services meet required minimum specifications.

Local authorities and RBCs will need to take a clear lead in this area, but it is logical for schools and colleges to develop their own individual policies based on their local requirements.

The NEN will also provide a stimulus for the development of innovative interactive content, in that it provides a robust and reliable delivery mechanism able to support services such as video conferencing and high-bandwidth content and applications. The development of a strategic approach to content hosting and delivery will help to ensure that the range of opportunities the NEN offers for learners and teachers can be fully exploited and that all content is appropriate, reliable and secure.

Authentication and authorisation

The work of Becta and its partners has shown that a unified authentication and authorisation infrastructure is needed to be able to meet the educational requirements outlined by the digital strategy and the development of the NEN. Becta's research has shown that Shibboleth is the most suitable solution for the education sector for accessing online content securely, and should be adopted as an integral component in the strategic approach to the future development of ICT in education, skills and children's services.

Shibboleth is an authentication system based on open-source software developed by the internet community with assistance from the National Science Foundation. It is essentially a transport mechanism built on top of an organisation's existing information that allows it to exchange information about its users in a secure and privacy-preserving manner.

Pilots indicate that Shibboleth-compliant technology will work within the complexity of the schools sector and external evaluation has also found that it is scalable for a national solution. Becta is now working with stakeholders and partners on developing the best way to implement Shibboleth nationally. More information can be found on the Becta website[30].

Solutions such as Shibboleth should be embedded within a wider strategic approach to security.

[29] See Becta Accreditation of Internet Services to Education scheme [http://ispsafety.ngfl.gov.uk]

[30] See Becta Technical policy and standards: Shibboleth – a strategic approach to school web content authentication and authorisation [http://www.becta.org.uk/schools/techstandards]





Organisational infrastructure specifications and accreditations

It is Becta's aim to help institutions to develop and maintain a coherent, sustainable and dependable ICT infrastructure by offering technical guidance and procurement advice. To facilitate this, it is vital for schools and colleges to have a vision for the infrastructure expressed in both functional and technical terms – of which e-safety must form a part.

Becta's functional specification[31] sets out Becta's vision for institutional infrastructure. It defines the vision primarily from a functional stance – providing a detailed view of what learners, educators and administrators should be able to expect from the institution's infrastructure and what functions must be in place in order to meet these expectations, under four functional requirements:

- Using ICT to offer a wide range of choice and access
- Using ICT to support flexible working
- Using ICT to manage data and improve efficiency
- Using ICT to secure data and protect the user.

The technical specification[32] recognises that a well-designed and well-maintained infrastructure is fundamental to an institution's ability to deliver a highly effective ICT resource to the learner, educator and administrator.

In order for the ICT infrastructure to be sustainable, flexible and adaptable, there needs to be a common approach to network design, ICT resources and security. A clear standards-based approach will help to ensure that infrastructures designed today are able to offer an ICT resource to the institution that is useful both today and in the future. In the document Becta addresses the technical specifications that underpin the functional requirements under four key areas of design criteria for institutions:

- Local area networks
- Services and applications
- Implementation of ICT security
- Network technologies.

The specification is an evolving document that we shall review at regular intervals. Please check the Becta website for the latest information.

Our recommendations for e-safety infrastructure and technology are therefore as follows:

- That local authorities and RBCs 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
- That individual schools and colleges develop a local implementation plan for filtering and monitoring use of the internet and communications technologies, and responding to violations (taking a lead from their local authority or RBC as appropriate with regard to both technical solutions and good practice)
- Recognising that it is a viable solution for the education sector, that Shibboleth be adopted for online resource authentication and authorisation, and to support the development of personalised online learning spaces for all learners.

[31] See Becta Technical policy and standards: Functional specification: Institutional infrastructure [http://www.becta.org.uk/schools/techstandards]

[32] See Becta Technical policy and standards: Technical specification: Institutional infrastructure [http://www.becta.org.uk/schools/techstandards]





Inspection, standards and ongoing assessment

Inspection of e-safety measures

Under Every child matters, children's services are to be inspected to ensure that the five outcomes are being met. Becta urges Ofsted to evaluate authority and organisational e-safety measures as part of this process.

The new Ofsted inspection framework[33] is based on self-evaluation, so it is important that all services aimed at children and young people have clear e-safety measures in place. These measures should be maintained and upheld at all times – not just to support the inspection process – and should go beyond purely technical solutions, providing policies and guidance on proactive actions for prevention and education in safe practices, reactive actions to incidents, and also procedures for dealing with disclosure.

Assessment of e-safety teaching

We have already identified the need to improve educational workforce confidence and competence in relation to e-safety issues, and for development in e-safety to form part of strategic leadership programmes. Practitioners and leaders should be assessed on their performance in this area, whether through national professional development frameworks or as part of the Ofsted inspection process.

Assessment of e-safety learning

We have previously discussed the need to embed e-safety teaching in the curriculum, and believe that it makes sense to assess awareness and understanding of the issues. Becta therefore urges awarding bodies to include assessment of staying safe online and digital literacy in appropriate qualifications.

[33] See Every child matters: The framework for inspection of children's services [http://www.ofsted.gov.uk/everychildconsultation]

With the move towards more online examinations and assessments, awarding bodies will also need to ensure that they have robust authentication systems in place to verify the identity of the learner, and that they have systems in place for detecting and responding to incidents of plagiarism or copyright infringement.

Ongoing assessment

Technology and safety issues are constantly changing, so there is a need to continually review advice and policy responses. It is also vital for institutions to have internal and, where appropriate, independent evaluations of the implementation of e-safety policy, along with a national view on how the numerous stakeholders are responding to the challenges. In addition, there is a requirement to benchmark e-safety resources systematically, evaluating their impact and ensuring that new resources, policy and campaigns are based on sound research and up-to-date information about social trends.

Our recommendations for e-safety inspection, standards and ongoing assessment are therefore as follows:

- That evaluation of e-safety measures be included as part of the inspection process
- That QCA review the position of e-safety awareness and digital literacy within its curriculum, assessment and regulatory frameworks
- That awarding bodies recognise e-safety issues and take steps to ensure that the examination process itself is safe, as assessment becomes increasingly dependent on ICT
- That research, evaluation and assessment into e-safety provision is on-going and appropriately funded and that Becta plays a strategic role in co-ordinating and reviewing this activity.





Summary and next steps

Becta hopes that this document will be a catalyst in helping to increase awareness of e-safety issues, at a time when the safeguarding of children is a high priority on political and social agendas.

In support of our recommendations Becta will:

- promote the report and its findings within the stakeholder community who have a duty of care to children
- actively engage with the specific organisations mentioned in this report to take our recommendations forward
- work with policy makers at national and local levels to ensure that appropriate e-safety recommendations are embedded into relevant documentation
- update all Becta advice and guidance in consultation with stakeholders and in line with the recommendations of this report
- continue to monitor e-safety issues that may arise as a result of new technological developments and advise our partner organisations accordingly.





Annex – The Safe Use of ICT in Education Steering Group

Becta would like to thank members of the Safe Use of ICT in Education Steering Group for their support in the writing and production of this publication.

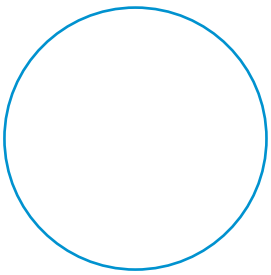
Chris Atkinson, NSPCC (seconded to CEOP)
Mary Barker, Naace
Ray Barker, BESA
Robin Blake, Ofcom
David Butler, NCPTA
Sue Butler, Learning and Skills Council
John Carr, NCH
Stephen Carrick-Davies, Childnet International
Andrew Cormack, Ukerna
Jim Donnelly, ASCL
Tony Fagelman, Internet Watch Foundation
Jim Gamble, CEOP
Richard Morrell, NTL, Virgin.net, Tesco.net
Rachel O'Connell, UCLAN
Stephen Ruddell, Home Office

The following organisations were consulted in the writing and production of this publication:

Department for Education and Skills (DfES)
Qualifications and Curriculum Authority (QCA)
Training and Development Agency for Schools (TDA)

Thanks also go to all the individuals and organisations that kindly provided feedback during the draft stages of this publication.




02/DD05-06/2038/116/NP/2k

Becta
ICT Advice

Millburn Hill Road
Science Park
Coventry
CV4 7JJ
Tel: 024 7641 6994
Fax: 024 7641 1418

Email: becta@becta.org.uk
URL: www.becta.org.uk