Schools

February 2009

Becta leading next generation learning

# AUPs in context:

## Establishing safe and responsible online behaviours

# Contents



## Disclaimer

We have made every effort to take into account relevant laws and best practice in the preparation of this publication. However, e-safety issues have the potential to be complex and multi-faceted and, as case law in this area is still very much under development, nothing in this publication should be deemed to constitute legal advice.

If you have a specific query relating to e-safety practice in your school or organisation, you should seek help from an appropriate adviser which may include your local authority (LA), children's services or local safeguarding children board (LSCB), child protection experts, the police, the Child Exploitation and Online Protection (CEOP) Centre, the Internet Watch Foundation (IWF), counsellors, legal advisers, the Department for Children, Schools and Families (DCSF) or others.

Becta (and other contributors to this document) can therefore accept no liability for any damage or loss suffered or incurred (whether directly, consequentially, indirectly or otherwise) by anyone relying on the information in this publication or any information referred to in it.

Inclusion of resources or references in this publication does not imply endorsement by Becta (or other contributors), nor does exclusion imply the reverse. URLs and information given in this document were correct at the time of publication, but may be subject to change over time.

# Section 1: About this document

In 2005, Becta published *E-safety: developing whole-school policies to support effective practice*, which provided guidance for schools on developing appropriate policies and procedures to ensure safe use of the internet by the children and young people in their care.

In Autumn 2008, Becta invited experts and practitioners[1] working in the field of e-safety to a series of working days with the aim of reviewing and updating the publication. This document is a reflection of current approaches to e-safety, and in particular, the role played by Acceptable Use Policies (AUPs) in maintaining safe behaviours online.

[1] See Annex D for a list of organisations represented at the e-safety working days.

# Section 2: The context for AUPs

"Children and young people need to be empowered to keep themselves safe – this isn't just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim."

Dr Tanya Byron
*Safer children in a digital world: The report of the Byron Review*[2]

In order to exploit the many educational and social benefits of new technologies, learners need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. At times, they will encounter risks.

We now recognise, however, that e-safety risks are posed more by behaviours and values online than the technology itself. Our approach must therefore shift: rather than restricting access to technology, we need to empower learners to develop safe and responsible online behaviours to protect themselves whenever and wherever they go online. AUPs, when embedded within a wider framework of e-safety measures (consisting of policies, infrastructure, education and standards[3]), can help to promote the positive behaviours needed. This, therefore, is the focus of this updated document.

There is also a wider imperative for schools and other children's services to develop effective AUPs.

The Byron Review investigated the issues and opportunities for keeping children and young people safe in their use of digital technologies, and the report, *Safer children in a digital world*, made a series of recommendations. A subsequent action plan[4], published in June 2008, sets out how these recommendations will be implemented under the direction of the newly established UK Council on Child Internet Safety (UKCCIS).

One of the strategic objectives of the review is to:

> *Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.*

[2] www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf

[3] Commonly referred to as the PIES model – see Section 4 for more detail on this approach.

[4] *The Byron Review action plan* www.dcsf.gov.uk/byronreview/actionplan

AUPs will clearly support this objective. Although primarily a tool for schools and other settings providing online services to children and young people, the key principles of the AUP can also be shared with parents and carers and provide a shared expectation of the behaviours children must adopt whenever, and wherever, they are using technology.

In her report, Dr Byron acknowledges that most schools already have AUPs in place (80 per cent of primary schools and 90 per cent of secondary schools according to previous Becta research[5]), but also states that there are indications that AUPs require regular refreshment to take account of the rapid advances of new technologies and children's applications. She also suggests that AUPs must promote positive uses of technologies, 'rather than just spelling out a list of "don'ts"'. As a result Dr Byron makes a series of recommendations regarding school approaches to e-safety, namely that:

> *... in all schools action is taken at a whole-school level to ensure that e-safety is mainstreamed throughout the school's teaching, learning and other practices. In particular I recommend that:*
>
> - *Government should encourage schools to use Becta's self-review framework[6] to drive continual improvement in schools' use of ICT including with regard to e-safety.*
> - *100 per cent of schools should have AUPs that are regularly reviewed, monitored and agreed with parents and students. Guidance on this should be incorporated in Becta's revised self-review framework.*

Dr Byron has also asked Ofsted to take various steps to hold schools to account for their performance in e-safety, including an increased emphasis on e-safety in the self-evaluation form (SEF)[7].

[5] Kitchen, S., Finch, S. and Sinclair, R. (2007) *Harnessing Technology schools survey 2007* www.becta.org.uk/research/reports/htlocalauthorities07

[6] See Annex A for more on the self-review framework.

[7] See Section 4 for more on Ofsted's role in e-safety inspection.

In the wider context of promoting greater use of technology for learning, in *Harnessing Technology: Next Generation Learning*[8] Becta outlines how it intends to secure a technologically confident education and skills system within England. The strategy aims to promote technology-related learner entitlement through a series of measures including family and informal learning, increased home access to technology, and enhanced parental engagement. Such initiatives will open up a whole range of new opportunities to children and their families, but we must also ensure that they are equipped to use them safely and responsibly.

Effective AUPs will become increasingly important as a tool to promote safe and responsible behaviours in using technology both at school and in the home.

This document therefore aims to help schools and other providers of education and services to children and young people to develop effective AUPs within a framework of wider e-safety measures, within their local context. It does not take a template approach, as to do so would diminish the value of the resulting document. Instead it provides a number of prompts and action points to help schools consider their local context for e-safety. We hope that you find it useful.

## Glossary of terms used in this document

**AUP:** Acceptable Use Policy. A document detailing the way in which new and emerging technologies may and may not be used and listing sanctions for misuse.

**Child:** Where we use the term 'child' (or its derivatives), we mean 'child or young person'; that is anyone who has not yet reached their eighteenth birthday[9].

**E-safety:** We use e-safety, and related terms such as 'online', 'communication technologies', and 'digital technologies' to refer to all fixed and mobile technologies that children may encounter, now and in the future, which might pose e-safety risks. We try to avoid using the term 'ICT' when talking about e-safety as this implies that it is a technical issue – which is not the case. The primary focus of e-safety is child protection: the issues should never be passed solely to technical staff to address.

[8] *Harnessing Technology: Next generation learning* www.becta.org.uk/publications/harnessingtechnologystrategy

[9] As defined in the *Children Act 1989* www.opsi.gov.uk/acts/acts1989/Ukpga_19890041_en_1.htm, the Children Act 2004 www.opsi.gov.uk/acts/acts2004/20040031.htm and various other safeguarding guidance

LSCB: Local Safeguarding Children Board. 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. LSCBs have an important role in overseeing e-safety approaches in the areas they serve.

PIES: A model for limiting e-safety risks based on a combined approach to policies, infrastructure and education, underpinned by standards and inspection[10].

Safeguarding: Safeguarding is defined for the purposes of this document as the process of increasing resilience to risks when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection. E-safety is just one aspect of a much wider safeguarding agenda within the UK, under the banner of *Every Child Matters: Change for Children*[11]. Those with responsibility for the development and delivery of e-safety policies should embed their work within the wider safeguarding agenda, and work across services to ensure that they are delivering the best possible opportunities for the children and young people in their care.

Schools: For ease of reading we refer predominantly to schools within this publication, but the underlying principles can be applied equally to any setting with responsibility for educating or safeguarding children and young people.

Users: We use this term, and related terms such as service users and end users, to mean those people who will ultimately be bound by the provisions of an AUP – this might be pupils, staff, parents and carers, or members of the wider community, depending on provisions of your AUP or the context in which you operate.

Web 2.0: Web tools and services which allow people to collaborate and share content online. Examples include blogs, wikis and social networking tools.

[10] See Section 4 for more on the PIES model for limiting e-safety risks.

[11] Every Child Matters website www.everychildmatters.gov.uk

# Section 3: Why are AUPs important?

Schools are increasingly recognising the benefits of technology – and particularly Web 2.0 technologies[12] – as an essential aspect of productive and creative social learning. However, in doing so they are finding that a blocking and banning approach which merely limits exposure to risk is no longer a sustainable approach. Children will experiment online, and while their confidence and enthusiasm for using new technologies may be high, their understanding of the opportunities and risks may be low, alongside their ability to respond to any risks they encounter. Schools now need to focus on a model of empowerment: equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks, wherever and whenever they go online. Effective AUPs can help to establish, and reinforce, safe and responsible online behaviours.

## Classifying the risks

The Byron Review classifies e-safety risks as involving **content, contact** and **conduct**, illustrating that the risk element involved in using new technologies is often determined by **behaviours** rather than the technologies themselves. A child may be a recipient, participant or actor in online activities posing risk, as illustrated in Figure 1.

| | **Commercial** | **Aggressive** | **Sexual** | **Values** |
|---|---|---|---|---|
| **Content** Child as recipient | Adverts<br>Spam<br>Sponsorship<br>Personal info | Violent/hateful content | Pornographic or unwelcome sexual content | Bias<br>Racist<br>Misleading info or advice |
| **Contact** Child as participant | Tracking<br>Harvesting personal info | Being bullied, harassed or stalked | Meeting strangers<br>Being groomed | Self-harm<br>Unwelcome persuasions |
| **Conduct** Child as actor | Illegal downloading<br>Hacking<br>Gambling<br>Financial scams<br>Terrorism[13] | Bullying or harassing another | Creating and uploading inappropriate material | Providing misleading info/advice |

Table developed by the EUKids Online project and referenced in paragraph 1.3 of the Byron Review.

Figure 1: Content, contact and conduct risks

[12] Becta has published a series of research on the use of Web 2.0 technologies for learning at Key Stages 3 and 4
www.becta.org.uk/research/reports/web2technologies

[13] The DCSF has recently released new guidance on preventing violent extremism. *Learning together to be safe: A toolkit to help schools contribute to the prevention of violent extremism*
www.dcsf.gov.uk/violentextremism/downloads/DCSF-Learning%20Together_bkmk.pdf

## Areas of concern

As the boundaries between the risks illustrated in Figure 1 become progressively blurred, the importance of positive online behaviours increases.

Social networking provides a good example of how online behaviour can present e-safety risks. This is extremely popular with children and young people, and encourages users to be creative users of the internet rather than just passive consumers. Users can express themselves with online personalities, chat and socialise with peers, and publish and share multimedia content such as music, photos and video clips with others.

If the basic e-safety 'rules' are followed, social networking poses little risk. However, if used inappropriately, many risks can be present for the user, and others:

- People may upload content that is inappropriate, offensive or even illegal to their online spaces, posting material that could damage their reputations or the reputations of others, or breach intellectual property rights. Posting inappropriate comments to the profiles of others can result in bullying or humiliation for the target, or potential charges of libel for the perpetrator.
- Although most social networking sites enable a profile to be set to private and only viewed by approved contacts, many users do not apply them. Maintaining very detailed online profiles, including personal information, photos and accounts of daily routines can lead to users being identified or contacted in person.
- Most social networking sites set age restrictions on using their services, but there is no way of authenticating users. As a result, many younger children disregard the terms and conditions of the service, unaware of the risks this might pose.
- Once posted online, a photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever. At its worst, in cases of online bullying, harassment or abuse, the inability to permanently remove online content and images can further add to the suffering of the target. Less damaging but equally impossible to remove, content posted in the naivety of youth could embarrass individuals in years to come.
- Young people have been known to post sexually explicit photos of themselves online, but those involved in such activities (or those forwarding such images to other recipients) could unknowingly be committing child sex abuse offences if the subject of the photo is, or appears to be, under the age of 18.

- Technology offers a perceived anonymity that may lead people to participate in abusive behaviours online that they would not contemplate in the real world. In cyberbullying, the target is potentially vulnerable 24:7 and no longer has a safe haven away from the bully; malicious or defamatory content can be circulated with ease, may be seen by a much wider audience, and will potentially exist forever despite best attempts to remove it.

Schools are ideally placed to embed a core set of e-safety skills from an early age, which will ultimately help protect children as they grow and mature, regardless of how the technology and risks evolve.

## Beyond children

Although we talk primarily about children when discussing e-safety, we must recognise that the development of safe and responsible online behaviours must extend much further – staff, parents and carers, and members of the wider community all have a role to play, and will all benefit from AUPs tailored to their particularly uses of technology.

Staff have a duty to protect the children in their care, but they are also susceptible to risks. There are many recent reports of teachers being harassed or intimidated using new technologies, both in and out of the classroom, and the DCSF Cyberbullying Taskforce, in consultation with the teaching unions and industry, is currently developing guidance in this area[14]. Equally, there are reported instances of childcare professionals compromising their professional reputation through social networking sites and other forms of media, or using school networks to access or circulate inappropriate or illegal content. Additionally, staff in schools and other children's services often have access to a range of sensitive and personal data, and must ensure that that they use technology and systems securely at all times (see Section 4 for more on this issue).

[14] Teachernet website
www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying


## Safe practice with technology

Kent County Council has produced a useful document for professionals working in schools.

Developed for teachers, volunteers, partner agencies and other school staff, it provides guidance on using technology as a communication tool in professional relationships, and understanding personal and professional boundaries, with the aim of protecting adults from misinterpretation of behaviour. It covers a range of technologies such as mobile phones, portable media devices and social networking.

For further information see Kent County Council e-safety pages www.kenttrustweb.org.uk?e-safety

Parents and carers are key to reinforcing positive and appropriate behaviours in their children, and will benefit from an awareness of the provisions of school-based AUPs. Additionally, with an increased focus on parental engagement, new issues may arise, and schools will need to be mindful of these as they implement their local policies. Parents for whom English is not their first language, those who have little or no literacy, or those who have little or no prior exposure to technology will need additional support in using the technology, and understanding both the benefits and risks.

Equally, there may be certain activities that parents and carers themselves are engaged in that may need to be addressed through an AUP. For example, a parent or carer might take a photograph or video at a school event featuring other children in addition to their own, and then post this to an online space such as a social networking site, naming every pupil. Aside from the general e-safety risks of making personal information available online, this may have particular implications if the image contains a vulnerable child. If they are aware of the issues and risks, and the rationale behind AUPs, parents and carers will be better placed to support and uphold them.

# Section 4: Where do we start?


Figure 2: PIES model for limiting e-safety risks

The PIES model (Figure 2) for limiting e-safety risks has been successfully adopted in many contexts. It offers a simple way of limiting risks through a combination of effective policies and practice, a robust and secure technology infrastructure, and education and training for both children and adults alike, all underpinned by standards and inspection.

This document focuses primarily on the policy element with a particular emphasis on developing effective AUPs, but the key features of each of the other elements are summarised briefly below. Other Becta resources deal with these in more detail (see Section 10 and Annex A).

## Policies and practices

Effective policies and practices can help to protect children and staff from e-safety risks, and promote safe and responsible use of technology wherever it occurs.

The policy aspect effectively contains three key areas:

- A detailed management document outlining the school's vision and approach to e-safety. This will include detailed descriptions of acceptable and unacceptable uses of technology and facilities, sanctions for misuse, procedures for responding to e-safety incidents, procedures for logging e-safety incidents and outcomes, and procedures for involving external agencies.
- A security and data management policy.
- A simple end-user AUP, to give users a clear understanding of what they can and can't do. It should be clear and concise, and written in a tone appropriate to the age and understanding of the users. It may be necessary to develop multiple versions of this document for various users – for example, pupils, staff, and parents and carers.

Some schools may choose to develop additional e-safety policies, such as stand-alone mobile phone policies, suited to their local context. E-safety messages must also be embedded within wider policies as appropriate, such as child protection, behaviour and anti-bullying policies.

## The differences between safety and security

While safety and security are very closely related and overlap in many regards, they are nevertheless two different concepts, which require different policies and technological approaches.

Ensuring safety encompasses technological approaches, for example, to protect users from inappropriate content and contact, and behavioural approaches, to encourage responsible and appropriate conduct. The best vehicle for this behavioural approach is a clearly communicated and regularly maintained AUP.

Similarly, ensuring security involves both technological and behavioural approaches. Technological measures are needed to protect the network and facilities from attack/compromise and inappropriate use (for example, appropriately configured and managed firewalls, anti-virus software and secure remote access facilities). In terms of user behaviours, policies should set out, for example, requirements for strong passwords and regular password changes. Such policies should also encourage and set expectations for user behaviour in relation to network and data security (for example, not sharing usernames and passwords).

Recent high-profile data security incidents have highlighted that awareness of security risks is in some instances not as high as it should be. To help address this, Becta has published data security guidance for schools, while Becta's functional and technical specifications for institutional infrastructure[15] and the FITS and FITS OM process frameworks[16], also provide assistance here.

Given these differences, some organisations find it useful to develop separate acceptable use and security policies to govern use of their ICT facilities. An additional security policy may be particularly appropriate for staff, to make their responsibilities when accessing potentially sensitive personal data explicit. If a single policy is employed, it is important to ensure that it addresses both security and safety issues as fully as possible.

[15] Becta website: Industry and developers: Standards and specifications
www.becta.org.uk/industry/techstandards

[16] Becta schools website
www.becta.org.uk/schools/fits

## Examples of e-safety and Acceptable Use Policies

The following sites provide examples of policies in all three of the areas discussed:

### Hertfordshire Grid for Learning
www.thegrid.org.uk/eservices/safety/index.shtml

Hertfordshire provides a range of information on school e-safety policies, including sample acceptable use agreements for primary schools, secondary schools, and staff, governors and visitors.

### Kent County Council
www.kenttrustweb.org.uk?e-safety

Kent has developed extensive e-safety policy guidance including guidance and templates for developing an e-safety policy, a core policy and audit document for both primary and secondary schools, and guidance on staff codes of conduct.

### Leeds Learning Network
www.leedslearning.net/resourcesandlinks/esafety.asp

Leeds Learning Network has developed various e-safety materials including an extensive guide to help schools develop their own AUP. The website also provides useful information on password security.

### London Grid for Learning
www.lgfl.net/lgfl/sections/safety/esafety/menu

The London Grid for Learning has developed a range of e-safety policy and strategy resources, including some good examples of differentiated AUPs for different user groups – primary children, secondary children and adults working in schools.

### Northamptonshire County Council
https://northants.lpplus.net/enable/e-safetyhome/pages/home.aspx

Northamptonshire provides a standard AUP which schools and other children's services can download and adapt to suit their individual setting.

### Northern Grid for Learning
www.northerngrid.org/esafety

The Northern Grid for Learning provides a range of information on AUPs, an e-safety audit tool and guidance on password protocols.

### South West Grid for Learning (SWGfL)
www.swgfl.org.uk/safety

SWGfL has developed a range of policy information including an AUP, an internet-safety protocol and various information on security policies.

**Staffordshire Safeguarding Children Board (SSCB)**
www.staffsscb.org.uk/e-safetytoolkit

SSCB have developed an online e-safety toolkit, providing information on Acceptable Use Policies, incident response, and roles and responsibilities.

**West Midlands Regional Broadband Consortium (WMnet)**
www.wmnet.org.uk/go/esafety

WMnet provides guidance on developing an AUP. They have also developed an e-safety framework as a tool that enables schools to assess and benchmark their adoption of good e-safety practice across all e-learning activities.

Please note: inclusion of resources in this section does not imply endorsement by Becta, nor does exclusion imply the reverse.

## Considering your legal powers

Sections 90 and 91 of the *Education and Inspections Act 2006*[17] provide new statutory powers for staff to discipline pupils for inappropriate behaviour or for not following instructions, both on and off school premises. Section 94 also gives schools the power to confiscate items from pupils as a disciplinary penalty.

These powers may be particularly important when dealing with e-safety issues: we know, for example, that online bullying may take place both inside and outside school, and so this legislation will give schools the legal power to intervene should incidents occur. It also gives teachers the power to confiscate mobile phones, and other personal devices, if they suspect that they are being used to compromise the wellbeing and safety of others.

Schools should consider their legal powers when developing e-safety policies and document sanctions for breaches of policy accordingly. The DCSF has produced a short guide[18] to help schools understand their powers under the provisions of the Act.

Your policies and practice must also reflect and complement those policies of the wider area, whether this is the local authority (LA), regional broadband consortium (RBC), or local safeguarding children board (LSCB). A cascading AUP model is discussed further in Section 8.

[17] OPSI website
www.opsi.gov.uk/acts/acts2006/ukpga_20060040_en_1

[18] DCSF website
www.dcsf.gov.uk/educationandinspectionsact/

### Action point:


The National Education Network (NEN) provides access to a free online e-safety tool, developed by the Northern Grid for Learning, to help schools and other educational establishments to check the status of e-safety provision, and to get advice and support on important e-safety issues.

Register with the site to check the status of your e-safety provision
www.nen.gov.uk/hot_topic

Actioned by: (insert name)
Date: (insert date)

### Action point:

Review the existing policies and practices in your school or service setting, and document these below. Do they cover both safety and security? Do they reflect your local setting? Are the policies regularly reviewed? Are there any gaps that need to be addressed? Use the results of the NEN e-safety audit you carried out above when reviewing your policies. The self-review framework (see Annex A) will also help you to review, and improve, your e-safety provision as part of your overall ICT effectiveness.

| Policy name: | Policy owned by: |
| --- | --- |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

## Infrastructure and technology

The technology infrastructure must be robust and secure, as it provides a 'first line of defence' against e-safety risks through tools such as firewalls, anti-virus software, content filtering and network monitoring systems.

Local needs will undoubtedly vary with regard to the requirements for technical solutions, but the Byron Review recommends that all schools and children's services use a Becta accredited internet service provider. Suppliers accredited through the scheme must meet and maintain specific standards in content filtering and service performance (see Annex A for further information).

Schools will also need to consider other technology factors such as procedures for proactive and reactive monitoring of the network (taking into account the rights of the network user), and network security and data management issues. The AUP should detail what monitoring is in place.

Actioned by: (insert name)
Date: (insert date)

| Last reviewed: | Next review due: | Comments: |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## The importance of good network practices

Good network practice is essential in protecting online privacy, minimising the risks of data security incidents and for complying with legislation.

Some basic ground rules for all network users can help maintain the security of data and systems. For example:

- passwords must be kept private
- strong passwords should be used – for example, a mixture of letters, number and keyboard characters; at least seven characters long and regularly changed
- workstations must be locked – or logged off – when left unattended
- all removable media must be virus checked before being used on the network
- all email attachments must be virus checked before they are opened
- personal login IDs should be used wherever possible (as opposed to a group profile); this can be particularly valuable in monitoring the technical infrastructure, allowing network managers to pinpoint exactly where and when problems have occurred.

Becta has developed guidance on infrastructure security including data security guidance for schools (www.becta.org.uk/schools/datasecurity)

Additionally, Get Safe Online provides a range of useful information, such as guidance on using strong passwords, aimed at a more general audience (www.getsafeonline.org)

**Action point:**

Check to ensure that your school or service setting is using a Becta accredited internet service provider. If it is not, consider the issues this raises... for example, does your service provider offer appropriate levels of filtering, blocking and monitoring? How do they respond to e-safety incidents? Does your position leave you vulnerable to increased e-safety risks?

Actioned by: (insert name)
Last reviewed: (insert date)
Comments: (insert comments relating to infrastructure provision)
Next review due: (insert date)

## Education and training

Education and training are essential for children and staff alike, providing an awareness of e-safety issues and risks, and strategies for dealing with them. With an increased focus on home access and parental engagement, using online tools, education and training will also be important for parents and carers too.

The methods used for the delivery of education and training will vary depending on your local context and audience. For example, the delivery of e-safety messages for younger children at Key Stage 1 will clearly be very different to e-safety messages delivered at Key Stage 4 and beyond, and likewise children with special educational needs or other vulnerabilities may need a different approach again. Staff may also have differentiated needs for e-safety education and training, and this should be reflected within personal professional development plans, while parents and carers may require a different approach entirely.

Any e-safety education programme must be continuous, providing information about new and emerging technologies as well as those already embedded within the culture of the school, responding to specific incidents and issues as appropriate.

There are a range of resources available to help deliver e-safety education and training, and the Becta guides, entitled *Signposts to Safety*[19], list a number of these. The Becta schools website also has a useful traffic lights activity[20] for introducing the concepts surrounding acceptable use, which can be easily adapted for use by children and adults alike

[19] See *Signposts to safety: Teaching e-safety at Key Stages 1 and 2* and *Signposts to safety: Teaching e-safety at Key Stages 3 and 4* www.becta.org.uk/publications/signpoststosafety

[20] See *E-safety: Introducing the concept of acceptable use in school* available via the Becta schools website www.becta.org.uk/schools/esafetyaup

How is e-safety education and training delivered within your organisation? Record your approaches below.

Actioned by: (insert name)

| Who: | Last reviewed: | Next review due: |
|---|---|---|
| Children and young people:<br>(insert comments relating to e-safety education and training provision for children and young people here) | | |
| Staff:<br>(insert comments relating to e-safety education and training provision for staff here) | | |
| Parents and carers:<br>(insert comments relating to e-safety education and training provision for parents and carers here) | | |

## Standards and inspection

The monitoring and evaluation of standards are essential in ensuring an e-safe environment, and can occur on many levels.

Schools and children's services should regularly review their e-safety provision in relation to emerging issues within the local context as well as national best practice. They should monitor and report on their e-safety provision, and maintain logs of e-safety incidents, resulting outcomes and follow-up actions taken. They should also be working with their LSCB to understand what is required of them in terms of the local area approach to safeguarding children online, including the type and frequency of reporting which is necessary at LSCB level.

The Byron Review has highlighted the value of two particular tools in supporting schools in reviewing their provision – the self-review framework and the Ofsted self-evaluation form.

### The self-review framework

The self-review framework (SRF), managed by Becta, is designed to help educational organisations to evaluate their use of technology in a structured way, and plan future improvements to learning and teaching through effective use of technology. E-safety elements are embedded within the framework as an essential component of such effectiveness. Further information on the approach is available in Annex A.

**Action point:**

If your school has not already done so, register with the self-review website (www.becta.org.uk/schools/selfreviewframework) to start exploring ways in which you can assess, evaluate and improve both your e-safety provision, and wider technology use.

Identify both strengths and weaknesses in your current e-safety provision, and develop an action plan.

Actioned by: (insert name)

Last reviewed: (insert date)

Comments: (insert comments relating to SRF findings)

Next review due: (insert date)

## Ofsted self-evaluation form

The Ofsted self-evaluation form (SEF)[21] forms the basis for school inspections. It allows schools to recognise their own strengths and weaknesses, and identify areas where they are trying to improve and develop.

In September 2007, Ofsted introduced a new prompt in the SEF specifically relating to e-safety. Question 4b reads:

*To what extent do learners feel safe and adopt safe practices? For example:*

- *whether learners feel safe from bullying, including any religious, racial (including Gypsy/Roma and Travellers of Irish heritage), sexual and homophobic incidents*
- *the extent to which learners have confidence to talk to staff and others when they feel at risk*
- *the extent to which learners adopt safe and responsible practices, dealing sensibly with risk, in a range of activities within and outside the classroom, including the use of new technologies and the internet.*

The Byron Review called on Ofsted to take various steps to hold schools to account for their performance in e-safety. As an initial response, Ofsted conducted an initial small-scale study of 100 self-evaluation forms in the summer of 2008[22].

[21] Ofsted website www.ofsted.gov.uk/Ofsted-home/Forms-and-guidance/Browse-all-by/Education-and-skills/Schools/How-we-inspect/School-self-evaluation

[22] *Safer children in a digital world: a response to the Byron Review request.* Visit www.ofsted.gov.uk and search on Byron Review to locate the document

A key finding was that around half of all schools surveyed failed to make any form of response on e-safety in their SEF, and a further quarter made only passing reference to it. Of the schools that did respond, the study found that there was considerable variation in how schools monitor and evaluate the effectiveness of their e-safety policies. A significant proportion of schools do not indicate how they know whether their policies are effective or not in ensuring learners' e-safety.

Ofsted's focus on e-safety will continue as the recommendations from the Byron Review are further implemented. All schools will need to actively monitor the impact of their e-safety policies and provide a comprehensive response to the SEF.

**Action point:**

Ensure that your school has provided a comprehensive response to question 4b on the Ofsted self-evaluation form. Monitor the impact of your e-safety policy at frequent intervals, revise policy and practice where necessary, and ensure that your SEF is regularly updated to reflect this.

Actioned by: (insert name)

Last reviewed: (insert date)

Comments: (insert comments relating to SEF response)

Next review due: (insert date)

# Section 5: Who needs to be involved?

In brief, everyone! E-safety is primarily a safeguarding issue, so anyone with responsibility for the welfare of children and young people needs to take responsibility for e-safety too. Children and young people themselves are integral to the process. They should be supported within an e-safe culture developed and maintained by both individuals and teams, both within an institution and beyond.

## Responsibilities of children and young people

The responsibilities of children and young people themselves should not be underestimated – they should be encouraged to develop their own sets of safe and responsible behaviours as, ultimately, this will provide the best defence for keeping them safe online. Responsibilities must be appropriate to the age, maturity and understanding of the child but, nevertheless, awareness should start at a very young age.

Children and young people should be encouraged to contribute to e-safety policies, for example, at school council meetings or through representative members on an e-safety team. If children feel that their views and opinions have been considered, and can understand some of the issues affecting the decisions documented in AUPs, they may be more inclined to abide by them.

In a school, pupil AUPs should be contained within the home–school agreement issued when a child commences their education at a particular setting – so introducing the concept of e-safety to parents and carers also. Additionally, pupils should be reminded of the terms of the AUP frequently, such as at the point of network login.

Key responsibilities for children and young people include:

- ☑ Contributing to the development of e-safety policies.
- ☑ Reading AUPs – and adhering to them.
- ☑ Taking responsibility for keeping themselves – and others – safe online.
- ☑ Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- ☑ Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.
- ☑ Respecting the feelings, rights, values and intellectual property of others.
- ☑ Seeking help from a trusted adult if things go wrong, and supporting others who may be experiencing e-safety issues.
- ☑ Discussing e-safety issues with parents and carers in an open and honest way.

## Responsibilities of the management team

The management team in a school or organisation have statutory responsibilities for child protection, of which e-safety is an aspect. It is imperative that the management team have a sound awareness of e-safety issues, and fully understand the importance of having effective e-safety policies and procedures in place. An e-safety governor should be appointed, and the management team must ensure that e-safety implications are duly considered within all other school business.

In practice much of the day-to-day responsibility for e-safety will be delegated to an e-safety team under the direction of a senior manager in the role of e-safety co-ordinator, but the management team must ultimately lead the e-safety vision and assign appropriate resources to deliver it.

The management team will need to take ultimate responsibility for any e-safety incidents which do occur, and lack of knowledge of the issues is no defence.

Key responsibilities of the management team include:

- ☑ Developing, owning and promoting the e-safety vision to all stakeholders.
- ☑ Supporting the e-safety co-ordinator in the development of an e-safe culture.
- ☑ Making appropriate resources available to support the development of an e-safe culture.
- ☑ Receiving and regularly reviewing e-safety incident logs.
- ☑ Supporting the e-safety co-ordinator in the appropriate escalation of e-safety incidents.
- ☑ Taking ultimate responsibility for e-safety incidents.

## The e-safety co-ordinator

An e-safety co-ordinator is crucial to the process of developing and maintaining an e-safe culture: a named individual with specific responsibility for overseeing each of the elements of the PIES model, ideally as part of a wider child protection role. Again we must stress that e-safety is not about ICT: it is not appropriate to delegate all responsibility to a member of the technical staff.

The e-safety co-ordinator must have the authority to call upon other staff within the organisation to assist them in their role: they may wish to convene an e-safety team with membership from all stakeholder groups to support the development and implementation of local policy and practice. The involvement of certain members of staff – such as child protection colleagues, SENCOs (special educational needs co-ordinators) and pastoral care staff – will be essential to ensure that safeguarding issues are considered from the widest possible perspective.

Key responsibilities of the e-safety co-ordinator include:

- ☑ Developing an e-safe culture under the direction of the management team and acting as a named point of contact on all e-safety issues.
- ☑ Leading an e-safety team with input from all stakeholder groups.
- ☑ Promoting the e-safety vision to all stakeholders, and supporting them in their understanding of the issues.
- ☑ Ensuring that e-safety is embedded within continuing professional development (CPD) for staff and co-ordinating training as appropriate.
- ☑ Ensuring that e-safety is embedded across the curriculum (or other learning activities) as appropriate.
- ☑ Ensuring that e-safety is promoted to parents and carers, and other users of network resources.
- ☑ Maintaining an e-safety incident log.
- ☑ Monitoring and reporting on e-safety issues to the management team, and other agencies as appropriate.
- ☑ Developing an understanding of the relevant legislation.
- ☑ Liaising with the local authority (or other local bodies) as appropriate.
- ☑ Liaising with other agencies as appropriate.
- ☑ Reviewing and updating e-safety policies and procedures on a regular basis.

## Responsibilities of staff managing the technical environment

Staff responsible for managing the technical environment have an important role to play in establishing – and maintaining – an e-safe environment.

All too often, the response to e-safety risks is to limit exposure through technical solutions such as a blocking or filtering approach. Although this undoubtedly has a place in some settings or situations, it does not lead to an e-mature outlook. Staff with responsibility for the technical environment should work closely with the management team, e-safety co-ordinator and curriculum staff where appropriate, to ensure that learning opportunities are not restricted by technical safety measures.

Technical staff will need support in their roles, and will require regular training to remain up to date with emerging e-safety issues. They should be clear about the procedures they must follow if they discover, or suspect, e-safety incidents through monitoring of network activity.

### Framework for ICT Technical Support

Becta has developed the Framework for ICT Technical Support (FITS)[23] which includes incident management – a process for logging, recording and resolving general ICT incidents. Although aimed primarily at schools, this may be a useful starting point from which to develop a process for responding to e-safety incidents for all children's services.

[23] Becta schools website
www.becta.org.uk/schools/fits

Key responsibilities for technical staff include:

- ☑ Acting as a key member of the e-safety team, supporting the e-safety co-ordinator in the development and implementation of appropriate e-safety policies and procedures.
- ☑ Providing a technical infrastructure to support e-safe practices, as appropriate to the local context, while ensuring that learning opportunities are still maximised.
- ☑ Taking responsibility for the security of systems and data.
- ☑ Reporting any technical breaches to the e-safety co-ordinator, and taking appropriate action as advised.
- ☑ Developing an understanding of the relevant legislation as it relates to the technical infrastructure.
- ☑ Liaising with the local authority (or other local bodies) as appropriate on technical infrastructure issues.
- ☑ Liaising with other agencies as appropriate.
- ☑ Reading staff AUPs – and adhering to them.
- ☑ Maintaining a professional level of conduct in their personal use of technology, both within and outside school.
- ☑ Taking personal responsibility for their professional development in this area.

It is recognised, however, that the resource available in a technical capacity will vary considerably between different settings, and that this may not always be a dedicated role. Where technical support has been outsourced to an external service provider, it is important that the service provider understands, supports and upholds your e-safety practices. They must take appropriate steps to minimise e-safety risks, and report any breaches of system or network security to the e-safety co-ordinator to enable appropriate internal action to be taken.

## Responsibilities of staff delivering the learning or care

Staff delivering the learning or care are essential to creating an e-safe culture, and typically have high levels of contact with the children and young people in their care and know them well.

Such staff may typically be the main channel for delivering e-safety education; they may be the first point of contact should e-safety incidents occur; or may be best placed to identify changes in behaviour that may indicate that a particular individual is at risk from e-safety issues. It is essential, therefore, that they have a good awareness of the issues, and know the appropriate procedures for escalating e-safety incidents or concerns.

It is also important that such staff model positive behaviours when using technologies in the learning or care environment, and adhere to staff AUPs.

### Key responsibilities for teaching and support staff include:

- ☑ Contributing to the development of e-safety policies.
- ☑ Reading staff AUPs – and adhering to them.
- ☑ Taking responsibility for the security of systems and data.
- ☑ Having an awareness of e-safety issues, and how they relate to the children in their care.
- ☑ Modelling good practice in using new and emerging technologies, emphasising positive learning opportunities rather than focusing on negatives.
- ☑ Embedding e-safety education in curriculum delivery wherever possible.
- ☑ Identifying individuals of concern and taking appropriate action.
- ☑ Knowing when and how to escalate e-safety issues.
- ☑ Maintaining a professional level of conduct in their personal use of technology, both within and outside school.
- ☑ Taking personal responsibility for their professional development in this area.

## Responsibilities of the wider community

Responsibilities of the wider community within the school – such as non-teaching staff, lunchtime staff, community volunteers, or other adults who may come into school on a more ad hoc basis – will be much the same as those staff delivering the learning or care. Disclosure of an e-safety incident can come at any time – at lunchtime in the playground, at an after-school club, or at a library or youth club – hence all adults working with children and young people have a duty to be aware of e-safety issues, and the appropriate procedures for response and escalation.

### Key responsibilities of the wider community include:

- ☑ Contributing to the development of e-safety policies.
- ☑ Reading staff AUPs – and adhering to them.
- ☑ Taking responsibility for the security of systems and data.
- ☑ Having an awareness of e-safety issues, and how they relate to those children in their care or with whom they have contact.
- ☑ Modelling good practice in using new and emerging technologies.
- ☑ Identifying individuals of concern and taking appropriate action.
- ☑ Knowing how and when to escalate e-safety issues.
- ☑ Maintaining a professional level of conduct in their personal use of technology, both within and outside school.
- ☑ Taking personal responsibility for their professional development in this area.

## Responsibilities of parents and carers

Parents and carers can play a critical role in developing safe and responsible online behaviours, and schools have a responsibility to work with them to raise their awareness of the issues. Through this approach, parents and carers can help to reinforce the e-safety messages delivered in schools, and promote and encourage e-safe behaviours wherever, and whenever, their children use new and emerging technologies.

Parental engagement strategies are set to enhance parental relationships with schools over the coming years. The development of learning platforms will mean that parents and carers will have real-time access to information about their child via the school network, and schools must ensure that parents and carers are aware of the safe and appropriate use of such systems. Equally,

strategies to increase access to learning from home will require adequate information and training for parents and carers who may have limited awareness of both the opportunities and risks of technologies. Schools, along with other agencies, must support parents and carers in their learning journey to ensure that they, in turn, can support their children in accessing the best possible learning opportunities with minimal risk. There is further information on these strategies in Annex A.

Parents and carers should also be encouraged to contribute to e-safety policies: if they understand the issues affecting the decisions documented in an AUP, they will be better placed to support them.

AUPs should be included within the home–school agreement along with other key documents (such as a digital image consent form) to ensure that parents and carers are aware of the provisions of the AUP, and the rules by which they and their children are expected to abide.

### Key responsibilities of parents and carers include:

- ☑ Contributing to the development of e-safety policies.
- ☑ Reading AUPs, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- ☑ Using learning platforms, and other network resources, safely and appropriately.
- ☑ Discussing e-safety issues with their children, supporting the school in its e-safety approaches and reinforcing appropriate behaviours at home.
- ☑ Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- ☑ Modelling appropriate uses of new and emerging technology.
- ☑ Liaising with school if they suspect, or have identified, that their child is conducting risky behaviour online.

# Section 6: What should an AUP include?

In Section 4 we described how an e-safety policy should cover three key areas:

- A detailed management document outlining the school's vision and approach to e-safety.
- A security and data management policy.
- A simple end-user AUP, distilling the key messages from both of the above to give users a clear understanding of what they can and can't do, how their use will be monitored, and sanctions for misuse.

This section focuses specifically on the third of these areas, outlining some general principles and suggestions for developing an effective AUP.

## General principles

There are some general principles that an effective end-user AUP should follow. For example, an AUP should:

☑ Be clear and concise.
A lengthy AUP will not be read or understood. Try to keep an AUP clear and concise – aim for a page or two of A4 of core rules for the day-to-day document, perhaps providing more detail in a supplementary document that could be issued as part of the home–school agreement or induction programme. The separate detailed management document should provide the necessary depth and detail needed by the e-safety co-ordinator and management team to create and maintain an e-safe culture.

☑ Reflect your setting.
The AUP must be relevant to your setting. Think through the issues in depth when creating your AUP, and model your approach on the needs and characteristics of your users, services and support networks. Consider your other policies – such as child protection, anti-bullying and behaviour policies – and ensure that your AUP reflects these and vice versa.

☑ Encourage end-user input.
If end-users feel they have ownership of the policy, they may be more likely to adhere to its contents. Involve children and young people, parents and carers, as well as those who are expected to enforce the policy, when developing and reviewing your AUP.

- ☑ **Be written in a tone and style that is appropriate to the end-user.**
  It may be necessary to develop several AUPs for different end-users within any one setting – for example, different documents for pupils, staff, and parents and carers, or those with particular communication needs. Again, it would be useful to have end-user input from each group to ensure that the final document meets their needs and can be fully understood. Some of the sample AUPs referenced in Section 4 provide good examples of documents created for different users.

- ☑ **Promote positive uses of new and emerging technologies.**
  Despite the risks, technology offers many wonderful opportunities: promote the positives in your AUP rather than focusing on the negatives. Remember also that technologies are evolving all the time: try to reinforce the concept of safe and responsible behaviours rather than focusing on specific technologies.

- ☑ **Clearly outline acceptable and unacceptable behaviours when using technology and network resources provided by the school.**
  End-users need a clear understanding of what they can, and can't do, online using the technology and services available to them in school.

- ☑ **Clearly outline acceptable and unacceptable behaviours when using personal technologies on school premises or networks.**
  End-users need a clear understanding of how they can use their own technology in certain settings. Strategies may range from a complete ban on all personal technologies, to approved use in certain situations, to positive encouragement of personal technologies to support and enhance the learning experience.

- ☑ **Clearly outline what network monitoring will take place.**
  End-users have a right to know how their network access will be monitored. An open and honest approach can help to prevent challenges to authority should e-safety incidents occur.

- ☑ **Clearly outline the sanctions for unacceptable use.**
  End-users need a clear understanding of the penalties they face if they break the rules. This may range from temporary suspension of services, to disciplinary action or even legal intervention, depending on the seriousness of the incident.

- ☑ **Be regularly reviewed and updated.**
  AUPs must be regularly reviewed and updated. This is essential if they are to remain effective in protecting children and young people, parents and carers, and staff and organisations from risk. In addition to a regular programme of review, AUPs should be reviewed more frequently if emerging issues or serious incidents dictate.

- ☑ **Be widely, and regularly, communicated to all stakeholder groups.**
  End-users need to be aware of the AUP – and understand it – if they are to adhere to it. Consider the best approaches for introducing the AUP: in a school this might be through the home–school agreement for pupils and parents or carers, or within induction programmes for staff – remember also to look for opportunities to assess whether it is understood. Reinforce the AUP regularly, monitor its impact and ensure that any changes in policy are also communicated to all those that need to know.

## Core AUP statements

Although AUPs should reflect the local context, there are core statements or approaches which all settings are likely to want to adopt and adapt as appropriate to the end-user's age and understanding. For example:

- All users must take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally.
- All users must be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.
- No communications device, whether school provided or personally owned, may be used for the bullying or harassment of others in any form.
- No applications or services accessed by users may be used to bring the school, or its members, into disrepute.
- All users have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others.
- All users have a duty to respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
- All users have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
- All users have a duty to protect their passwords and personal network logins, and should log off the network when leaving workstations unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- All users should use network resources responsibly. Wasting staff effort or networked resources, or using the resources in such a way so as to diminish the service for other network users, is unacceptable.
- All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- All users should be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to check and/or confiscate personal technologies such as mobile phones.

- All users must take responsibility for reading and upholding the standards laid out in the AUP.
- All users should understand that the AUP is regularly reviewed and consistently enforced.

The AUP should also:

- provide information on where users can access material, advice and guidance relating to e-safety issues
- provide information on what sanctions may be taken if the AUP is not followed.

### Presenting an AUP

Think about how best to present the AUP in a style and tone that is appropriate to the intended audience.

Remember, the AUP is a vehicle for protecting the institution as well as the individual, to articulate what it will and won't do to help keep users and systems safe and secure. For example, just as the individual should undertake not to share usernames and passwords with others, the institution should explain how the use of facilities will be monitored and how users' personal information will be kept secure.

One presentational approach could be:

- What you can do...
- What you cannot do...
- What we will do...
- What we won't do...

## Additional AUP statements

The core AUP statements outlined should apply to all user groups, whether children, staff, or parents and carers. However, additional provisions may be necessary for particular user groups as appropriate to their age and understanding, or roles and responsibilities, or for particular settings.

For example, a school might take a particular approach to the use of personal technologies on both its premises and network, and so will need to document this within its AUP. Indeed it might have differentiated approaches for pupils in different year groups, or for staff use of personal technologies, and this should be made clear within the relevant end-user AUP.

A staff AUP may have extra provisions for their responsibilities relating to the safety and security of data, and particularly the transfer of data between systems and locations using removable media. It might also contain statements relating to the professional conduct that staff are expected to abide by when using technology both in and out of school.

An AUP for parents and carers, on the other hand, may include particular provisions relating to parental engagement initiatives. For example, if access to a learning platform is given, the AUP may include clauses that only information pertaining to their child may be accessed, and that network resources may not be copied or used outside of the learning platform.

Further information is given in the next section on issues relating to specific settings.

Remember, if you have a specific query relating to e-safety policy or practice in your school or organisation, you should seek help from an appropriate legal adviser.

# Section 7: What are the issues for specific settings?

Effective e-safety policies must reflect the local context. The following sections suggest some considerations that might have a particular bearing in specific contexts.

## Early years settings

Children are encountering a variety of technologies at ever younger ages, and so their e-safety education must start at an early age also. Even though very young children may be starting to access technology independently, and be familiar with a wide range of technologies, it is essential that positive behaviours are introduced from the outset, in ways appropriate to their level of understanding.

E-safety and AUPs will also need to consider other uses of technology in such settings – for example, a nursery that provides webcam access for parents to check up on their child's day will need to consider the e-safety issues should access to the webcam be compromised, while staff may need clear guidance on procedures for taking, using and storing digital images for use within classroom displays.

Early years settings also present a good opportunity to introduce the concept of e-safety to parents and carers – if they can gain an awareness and understanding of the issues while their children are still very young, they will be better placed to support and learn with them as they encounter more technology, and hence increased risk.

## Primary schools

Primary schools offer a supervised environment where there is typically a clear focus for technology use in the classroom and directed activities. However, we know that children are using technology at an increasingly younger age, and there is a risk that their experiences and access to technology outside school may exceed the experiences and access within it. Primary schools must therefore play a key role in helping children develop e-safety skills from an early age.

Staff within primary settings will typically know their pupils very well, and may be best placed to identify any emerging issues or concerns. Additionally, primary schools will have a high level of access to parents and carers, providing a good opportunity to introduce, or strengthen, e-safety awareness and understanding, and work with them should issues arise.

National initiatives focusing on home access and parental engagement will strengthen opportunities for primary schools to work with parents and carers to promote an e-safe culture.

## Secondary schools

By secondary school, students' independent access to technology will be greater still, and they are likely to have access to a range of personal technology devices. They may be using technology extensively outside school, and their access, knowledge and awareness of specific technologies may outstrip that of teaching staff. However, while their apparent confidence in using technologies may be high, their competence may be less so! They may also be engaging in more risky and experimental behaviours, both online and offline, which is a natural feature of growing up.

E-safety education should be firmly embedded within the curriculum at secondary level, but the lack of contact time with any one teacher may make it more difficult to identify young people at risk. A co-ordinated approach to reporting and managing e-safety incidents across a secondary school is essential.

Typically, secondary schools may have less access to parents and carers through which to share e-safety messages but, as with primary schools, the home access and parental engagement initiatives will provide new mechanisms to strengthen communication.

## Home access and parental engagement

The focus on home access and parental engagement is set to develop significantly in coming years. There are several key considerations.

Under the home access initiative, online learning opportunities will become increasingly available to all homes[24] encouraging all families to develop learning and skills online[25]. First and foremost, parents and carers need to understand the many positive educational opportunities that this will bring to their children and the wider family, but they will also need to understand how to keep their children (and themselves) safe online. The process must be carefully managed to offer parents and carers practical advice and guidance on using technology safely and responsibly, without being alarmist.

Parental engagement initiatives will encourage parents and carers to access information and resources online to support their child's education, and again the process must be carefully managed. The security of data and networks must be carefully considered, with robust and secure authentication methods, and clear guidelines on the appropriate (and inappropriate) uses of the resources and facilities on offer.

[24] Further information on the Home Access scheme is available from Becta www.becta.org.uk/homeaccess

[25] You can find out more about the Next Generation Learning campaign from Becta www.becta.org.uk/nextgenerationlearning

## FE and skills settings

Further education (FE) and skills settings can offer a number of challenges for e-safety, mainly due to the diversity of the sector.

The 14–19 agenda offers new flexible ways for delivering education, and learners may receive their education from multiple locations, each with different technologies, and each with different rules governing its use. Work-based learners, on the other hand, will still be covered by the duty of care of their learning establishment, but will typically have access to a more business-orientated technology environment, which may have fewer safeguarding controls in place.

Typically, learners in FE and skills settings will require a more mature approach to e-safety, and the tone and language of AUPs should reflect this.

Becta, in conjunction with the Department for Innovation, Universities and Skills (DIUS), and other partners from the FE and skills sector, is developing additional guidance in this area. See the Becta FE and skills portal for further information (http://feandskills.becta.org.uk).

## Children with special educational needs or particular vulnerability

The *Staying Safe Action Plan*[26] identifies that targeted safeguarding is needed for some groups of children who are at greater risk than others, and it is important to target policies and services to these groups to help keep them safe from harm. This might include children and young people with special educational needs, mobile or travelling children, children for whom English is an additional language, those in hospital, residential, or special schools, children in pupil referral units, or those in care.

Children in these groups may be particularly vulnerable to e-safety risks. To give some examples:

- Levels of understanding: degrees of general learning difficulty (and how these interact with maturity) will determine how far children are aware of the social and other implications of the content of their communication – both in expression and in making sense of communication received. There may be a discrepancy between both the maturity and the learning difficulties of the sender of messages and the recipient, and vice versa. Certain forms of special need, such as autism, may result in children making particularly literal interpretations of content, which will affect the sense they make of communications.
- Understanding of technology: vulnerable children may also misjudge communication and be unaware of how widely messages may be disseminated. They may also have difficulty in appreciating the need to restrict access to personal information or use of personal videos, for example.
- Language barriers: those new to English may not be familiar with the social implications in the use of language, and the same may apply to their parents.
- Physical or sensory disabilities: children and young people with physical or sensory disabilities may be attracted by the anonymity of communication, and the scope for incognito presentations of themselves. The 'unreality' to which this gives rise may have unfortunate consequences.
- Emotional and behavioural difficulties: children with emotional and behavioural difficulties may well express these in their communications and may not allow for the effect this may have on the recipients – and on the response their communication evokes. This may lead to heightened emotional involvement with unrealistic expectations as a consequence.

[26] http://publications.teachernet.gov.uk/eOrderingDownload/DCSF-00151-2008.pdf

- Settings: children in restricted settings with high levels of supervision are likely to be protected from some of the more obvious risks. Consequently, they may not be aware of risks in using technology in non-restricted settings such as their own homes, internet cafes or libraries and may not be well equipped to respond to these.
- Supervision: those responsible for supervision in settings must be aware of the very real dilemma they face in balancing their concern to protect children from risk with their obligation to recognise children's rights to express themselves and interact with their peers and others. This particularly applies as children get older.

In particular, difficulties may arise in relation to learners being advised not to disclose their passwords but needing assistance to use, or remember, them, and the need to exercise a duty of care. Those responsible for delivering services to children with special educational needs or particular vulnerabilities are best placed to understand the unique characteristics of those in their care, and should carefully consider their specific needs with regard to e-safety.

### E-safety and looked-after children

A recent report by the Children's Rights Director for England, *Future care: Children's advice on future care standards*, asked children for their views on future standards for services that look after children. Children were asked for their views on internet safety, and gave three very clear messages that need to be taken into account for future standards:

- Unsuitable or dangerous sites and chatrooms should, if possible, be blocked so that children cannot get on to them.
- The best way of keeping children safe on the internet is for adults to supervise how they are using it.
- Children, especially younger children, need to be taught the basics about internet safety and how to keep themselves safe.

The children also suggested a number of rules for staying safe on the internet, many stating that 'it was then up to them as young people to keep to these rules'.

The full report is available to download from the Ofsted website. Visit www.ofsted.gov.uk and search on Future Care to locate the document.

## Other LSCB services

A wide range of children's services come under the jurisdiction of the LSCB, and the characteristics of each will vary greatly. Such services will need to consider the age and understanding of their users, the awareness and understanding of staff, the access to and levels of supervision when using technology, and the technological controls in place, among other factors.

Becta has been working with LSCBs to support them in developing an e-safety strategy across all of their services. Each LSCB should have appointed an e-safety strategy lead to co-ordinate local activity, and will be developing protocols for local incident handling, ensuring consistency of approach across all services to children within their remit. It is essential that all children's services are familiar with the e-safety procedures of their LSCB, and know who to contact for further advice and support.

# Section 8: What's the bigger picture?

When developing your AUP, consider the bigger picture. Find out what policies are already in place through your LA, regional broadband consortium (RBC) (or whoever provides your internet connectivity) and your LSCB. By default, you may be bound by the terms of their AUPs, and will need to reflect this in your local policies accordingly.

## A cascading model for acceptable use

The NEN is the UK collaborative network for education, providing schools and other connected institutions with a safe, secure and reliable learning environment and direct access to a growing range of online services and content. The network is made up of regional networks maintained by NEN access providers (including the devolved administrations, local authorities and RBCs), with each interconnected by the SuperJANET technical infrastructure maintained by JANET (UK).

The NEN Safeguarding Group is developing a standard AUP template, building upon the provisions of the JANET (UK) AUP, based on a cascading model of acceptable use. Within this model, each layer in the cascade inherits a set of core requirements from the layer above to which it (and its users) must abide. In turn, further local requirements can be added. This is illustrated in Figure 3 below.

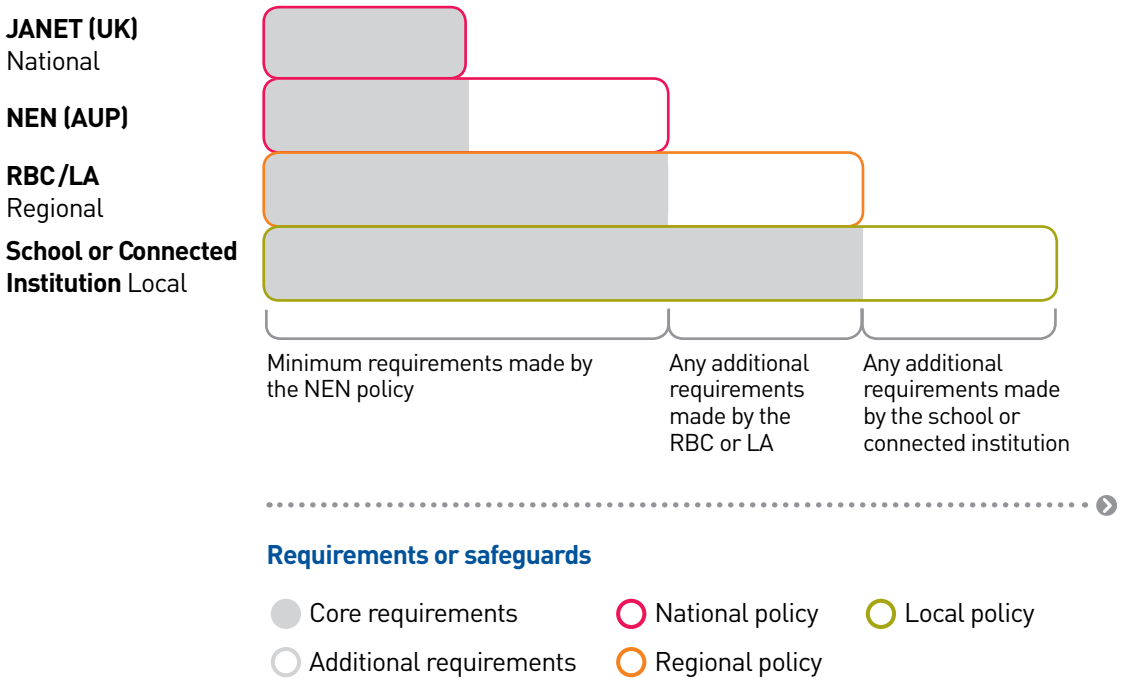



Figure 3: A national to local policy cascade for AUPs

In brief, within the NEN AUP, acceptable use will include any legal activity that furthers the aims and policies of a user organisation, furthers the learning or education of users, supports teaching, aids appropriate communication and supports administrative functions.

Examples of unacceptable use, although not exhaustive, will include any activity which may reasonably be regarded as unlawful, the creation or transmission of any inappropriate, offensive, obscene or indecent content, or the use of the network to bully or harass, defame, defraud, or infringe copyright. Additionally, the AUP will state that any deliberate misuse of networks and resources, such as attempts at unauthorised access to facilities and services, attempts to conceal network identities or otherwise evade safety and security controls, deliberately accessing, corrupting or destroying other users' data, compromising the privacy of others, or wasting staff effort or networked resources is unacceptable.

NEN access providers will be encouraged to build upon the provisions of the NEN AUP at a regional level, as appropriate to their individual business needs and the local communities they serve. Additionally, each user organisation should then establish its own statement of acceptable use within the context of the services provided to its users, ensuring that the conditions outlined in the AUPs further up the chain are implicit within local policy.

For further information, see the NEN website (www.nen.gov.uk)

**Action point:**

List the AUPs that relate to you and where you can access these:

- ☑ School. Location:
- ☑ Local authority. Location:
- ☑ LSCB. Location:
- ☑ RBC. Location:
- ☑ ISP. Location:
- ☑ Others. Type and location:

Actioned by: (insert name)

Last reviewed: (insert date)

Remember also that users will move between different settings when using technology and, as such, will need to adhere to the provisions of different AUPs. Awareness raising on this issue should form part of their e-safety education.

# Section 9: How do we deal with e-safety incidents?

Regardless of having the best e-safety policies and practice in place, there may still be occasions when e-safety incidents occur. Your end-user AUP will outline appropriate and inappropriate behaviours and sanctions for misuse, but your detailed e-safety management document must also contain clear guidelines for responding to e-safety incidents, and clear lines of communication for escalating specific incidents where necessary. Everyone must be aware of the process.

Escalation of incidents may take place within the school or other service setting, or may require the notification and disclosure to external agencies such as the LSCB, the police or another appropriate agency.

In developing your responses, you should consider various e-safety scenarios, responses and reporting mechanisms – for example:

- **Accidental or deliberate access to inappropriate material**
  The definition of 'inappropriate' may change according to your users or the setting. Your AUP should make clear what is deemed to be inappropriate material within your context, and the sanctions which will apply. Different approaches may be necessary depending on whether the access was accidental or deliberate.
- **Accidental or deliberate access to illegal material**
  If filters are correctly set, it should not be possible to access illegal materials. You should check your settings on a regular basis to ensure that they filter as expected, and the levels of filtering are appropriate for the end-user. If illegal material is accessed, escalation of the incident will be necessary.
- **Inappropriate use of email or other technologies**
  Again, the definition of inappropriate may change according to your users or the setting. Your AUP should make clear what is deemed to be inappropriate use of email and other technologies within the context of your setting and services, and the sanctions which will apply.
- **Illegal use of email and other technologies**
  Illegal use of email and other technologies should always be escalated to an appropriate agency.
- **Deliberate misuse of the network**
  (for example, hacking, virus propagation or circumventing safety controls)
  Your AUP should clearly state what is deemed to be inappropriate use of network resources, the monitoring that is in place and the sanctions which will apply to deliberate misuse. If networks have been used for illegal activity, the incident should be escalated accordingly.

- **Bullying or harassment using technologies**
  Bullying or harassment is not acceptable in any circumstance, via any means, and responses should mirror those documented in established anti-bullying policies. It may also be necessary to involve appropriate external agencies, depending on the severity of the event.
- **Sexual exploitation using technologies**
  This is a serious offence, and will require escalation to appropriate external agencies as necessary.

Depending on the nature of the event, different e-safety incidents will require different responses, and undoubtedly no two e-safety incidents will be exactly the same. This does not mean, however, that responses should be left to chance and circumstance: instead you should attempt to model general processes and procedures for responding to incidents as appropriate to your context, drawing on good practice within the wider field of child protection. Such exercises can often be effective as both awareness raising and training tools. Remember, incidents may involve children and young people, staff, or others as both victims and perpetrators, and your response model must be capable of dealing with each of these quickly and effectively.

In earlier e-safety publications Becta has modelled an outline flowchart for responding to e-safety incidents. This is reproduced in Annex B, along with a resource for identifying and mapping local contacts and support networks in Annex C. Schools, and other children's services, may wish to consider similar approaches for defining their own response procedures.

We also recommend that schools and children's services make contact with their LSCB to establish the procedures in place at a regional level, to ensure that their own policies reflect regional practice.

# Section 10: Where can we get further help?

E-safety is not something that schools and children's services need to face in isolation. There are many opportunities to share good practice and learn from the experiences of others. This section suggests a few ideas for doing this.

## Becta resources

### Safetynet mailing list

www.becta.org.uk/schools/communities/safetynet

Safetynet is a mailing list specifically for anyone who wants to discuss and share information to support the development of e-safety good practice. The list is for educational practitioners, LAs, LSCBs and others who have an interest and/or responsibility in this area. It has been set up to provide:

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

Any updates or additions to information in this document, or additional opportunities arising from this strand of work, will be posted to this list.

Safetynet is an open discussion group. This means that anyone with an interest in e-safety is welcome to participate in the discussions. All discussions will be publicly available and when you post a message, your email address will be visible to registered users. Messages are archived online in the Becta Communities service, and may also be archived (and hence searchable) more widely through commercial search engines. The service is reactively monitored, and all participants are expected to adhere to the Becta Communities AUPs.

### Online resources

www.becta.org.uk

The Becta website aims to highlight e-safety issues relating to new technologies, and publish practical information and advice for schools, LAs and LSCBs on how to use those technologies safely.

We update the site regularly with information on emerging issues and technologies, and examples of good practice. Updates or additions to information in this document will be posted online.

### E-safety publications

www.becta.org.uk/publications

Becta has produced a number of publications on various aspects of e-safety. You may download all these titles as PDF files from the Becta publications website. Publications include:

- **Signposts to safety: teaching e-safety at Key Stages 1 and 2**
  This publication contains signposts to a selection of resources, along with appropriate curriculum links, to help teachers of Key Stages 1 and 2 to teach e-safety messages in the classroom.
- **Signposts to safety: teaching e-safety at Key Stages 3 and 4**
  This contains signposts to a selection of resources plus curriculum links to help teachers of Key Stages 3 and 4 to teach e-safety messages in the classroom.
- **Safeguarding children in a digital world: developing a strategic approach to e-safety**
  This publication offers 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 in a child's education. The guidance refers to policies and documentation for England, but the principles have resonance across the UK and beyond.
- **Safeguarding children online: a guide for local authorities and local safeguarding children boards**
  This contains a series of practical checklists for LAs and, more specifically, for LSCBs on developing a co-ordinated approach to e-safety across all services within their remit.

Further information on Becta's wider work is contained in Annex A.

## Cross-organisation working

Where possible, opportunities for cross-organisation working within the local area should be investigated. This can help to develop both strategy and practice, provide cohesion for children and young people as they move between services, and provide an effective framework for benchmarking and peer review. Examples might include a group of local primary schools working together to respond to emerging e-safety issues, secondary schools working with their feeder primary schools to establish the levels of e-safety awareness on transfer, or a consortium of settings involved in providing education and training under the 14–19 agenda working together to review issues relating to AUPs in different institutions.

As an absolute minimum, schools and other settings providing services to children and young people should make contact with their LSCB to establish the level of e-safety provision already in place at a regional level.

## Other sources of support and information

A selection of organisations providing e-safety support and information are detailed below.

### Child Exploitation and Online Protection Centre

www.ceop.gov.uk

CEOP is a police organisation focused on the protection of children and young people from sexual abuse and exploitation; it has a broad remit and range of functions to help tackle the sexual abuse and exploitation of children – primarily where use of technology is a factor, or media such as the online environment are utilised. It is also a founder member of the Virtual Global Taskforce (VGT), an international collaboration of law enforcement agencies committed to tackling this abuse of children and young people. Through its holistic approach, CEOP aims to learn from its work and that of others to ensure that measures are put in place to prevent or reduce harm to children and young people in the future; this includes the development and rollout of an education programme called Thinkuknow (www.thinkuknow.co.uk) for professionals to use with children and young people to help keep them safe online.

CEOP provides an online facility, in association with the VGT, for the public reporting of any sexually inappropriate or potentially illegal online activity towards a child or young person. For example, this might be an online conversation with someone who a child thinks may be an adult and who is engaging with that child in a way which makes them feel sexually uncomfortable, or exposing them to illegal or pornographic material, or who is trying to meet a child for sexual purposes. See the CEOP website for more information on the work of CEOP and how it could assist you.

*Where a child or young person may be in immediate danger, always dial 999 for police assistance.*

There are prominent reporting links from the CEOP website, the Virtual Global Taskforce website (www.virtualglobaltaskforce.com) and the Thinkuknow website. A reporting link is also available as a tab option in Windows Live Messenger.

### Know IT All
www.childnet.com/kia

Childnet International, a charity that is helping to make the internet a great and safe place for children, have developed a set of award-winning resources called Know IT All. The resources aim to help educate young people, parents, teachers and volunteers about safe and positive use of the internet.

### Internet Watch Foundation
www.iwf.org.uk

The Internet Watch Foundation (IWF) is the UK internet hotline for reporting illegal online content – specifically child sexual abuse images hosted worldwide and criminally obscene and incitement to racial hatred content which is hosted in the UK. The IWF works in partnership with the online industry, the Government, law enforcement agencies and other hotlines abroad to remove such content from the internet. A prominent link for reporting illegal content appears on the home page of the IWF website.

### ChildLine
www.childline.org.uk

ChildLine is a service provided by the NSPCC offering a free and confidential helpline for children in danger and distress. Children and young people in the UK may call 0800 1111 to talk about any problem, 24 hours a day.

The ChildLine service is delivered in Scotland by Children 1st on behalf of the NSPCC.

### National Education Network
www.nen.gov.uk

The NEN is the UK collaborative network for education, providing schools with a safe, secure and reliable learning environment and direct access to a growing range of online services and content. It features a range of e-safety tools and resources.

### Teachtoday
www.teachtoday.eu

Teachtoday provides resources for teachers on the responsible and safe use of new and existing communications technologies. Driven by Europe's leading internet, mobile network and social networking providers, working in partnership with European Schoolnet, Teachtoday aims to help schools:

- understand new mobile and internet technologies, including social networking
- know what action to take when facing problems
- find resources to support the teaching of positive, responsible and safe use of technology.

# Annexes

## Annex A: Other areas of Becta's work

A selection of Becta's wider work which is related to e-safety policy and practice, is detailed below.

### Accreditation of Internet Services to Education scheme

This scheme enables schools and other establishments to make an informed choice of internet service provider (ISP) or filtering solution. Accredited suppliers must meet and maintain specific standards in content filtering and service performance. The accreditation process is open to commercial providers and other organisations providing internet services, such as local authorities and regional broadband consortia.

The standards of assessment have been developed in consultation with partners in education and industry to ensure the provision of reliable and relevant information. The accreditation has undergone a recent review, and the scope of the scheme has now been extended to include a wider range of stand-alone products designed to protect internet users not just in the school environment, but which can also be employed in other environments where children and young people have access to the internet. The process makes a technical assessment of content filtering services provided by ISPs and stand-alone product providers for factors such as browsing of web-based content, email filtering, blocking and filtering of newsgroups and chat services, and virus alerting, all with a strong focus on e-safety.

Assessments of service options such as customised filtering for different user groups are also made, and minimum requirements for factors such as uptime, connection speeds and service support are also defined.

For further information see www.becta.org.uk/schools/ispsafety

## Framework for ICT Technical Support

Becta's Framework for ICT Technical Support (FITS) aims to provide a reliable and effective ICT infrastructure. There is a separate toolkit for primary and secondary schools to help them implement the framework.

The primary toolkit is for primary schools or schools that rely on an external provider for the majority of their ICT management and support.

The secondary toolkit is for schools that have an internal ICT support team for the majority of their ICT management and support.

FITS Operations Management (FITS OM) is a new framework for schools that have implemented the FITS processes and would like to improve the operations management.

For further information see www.becta.org.uk/schools/fits

## Home Access

Access to technology at home benefits learners in a range of different ways. It can improve learning and achievement, motivate and engage children, and encourage independence and creativity. It can also help to connect learning at school and at home, and can help parents and carers get more involved.

The Government's vision is to ensure that all pupils aged 5–19 in state maintained education in England, have the opportunity to have access to computers and internet connectivity for education at home. A £300m Home Access programme, managed by Becta, will help to achieve this vision. Pilots commenced early in 2009 and the scheme will be rolled out nationally in the autumn.

Findings from the pilot will help to inform additional e-safety guidance for schools and families as the programme rolls out further.

For further information see www.becta.org.uk/homeaccess

## Parental engagement

Providing parents and carers with timely and meaningful information about their children's school lives and work can help raise learner achievement. Technology can help this process by enabling parents and carers to receive and access information about their children's work, progress, attendance and behaviour when and where they want using, for example, secure online or even mobile access. This idea is outlined in the Government's *The Children's Plan*[27].

All secondary schools are expected to make a range of information available to parents and carers via secure online access by September 2010. Primary schools are expected to achieve this by 2012.

For further information see www.becta.org.uk/engagingparents

## Self-review framework

The self-review framework is designed to help educational organisations to evaluate their use of technology in a structured way, and plan future improvements to learning and teaching.

Based on educational research and tried and tested methods for supporting school improvement, the self-review framework offers schools a straightforward route for improving their effective use of technology. It also offers benchmarking against established best practice and helps schools to ensure that their ICT infrastructure meets their needs, not only now, but in the future.

The framework consists of eight elements, further divided into strands and aspects. Each aspect contains a series of indicators which describe a level of maturity. An online tool helps schools to develop a profile of their current position and future actions, providing tools to link evidence to the evaluations.

There are many benefits of working through the framework, including:

- helping to ensure that investment in ICT is fit for purpose
- offering a straightforward process for identifying strengths and weaknesses
- developing a deeper understanding of the school's vision for ICT by involving a wide range of staff in the process

[27] *The Children's Plan: Building brighter futures* www.dcsf.gov.uk/publications/childrensplan/downloads/The_Childrens_Plan.pdf

- encouraging commitment and involvement from the whole school
- helping set and achieve realistic goals for improvement
- adding value to your engagement with other educational initiatives such as the National Strategies, extended schools and Every Child Matters
- complementing the Ofsted self-evaluation form (see Section 4).

Additionally, the levels of progress through the framework can be recognised through the Next Generation Learning Charter[28].

E-safety elements are embedded within the self-review framework as an essential component of ICT effectiveness. Schools and educational establishments are encouraged to use the tool as part of their overall e-safety strategy. While the self-review framework is not designed with wider children's services in mind, such organisations might like to consider the underlying principles to support their own approaches to the effective use of technology in their own service settings.

For further information, and to register for an account to use the online tool, please see www.becta.org.uk/schools/selfreviewframework

## Annex B: Flowchart for responding to e-safety incidents

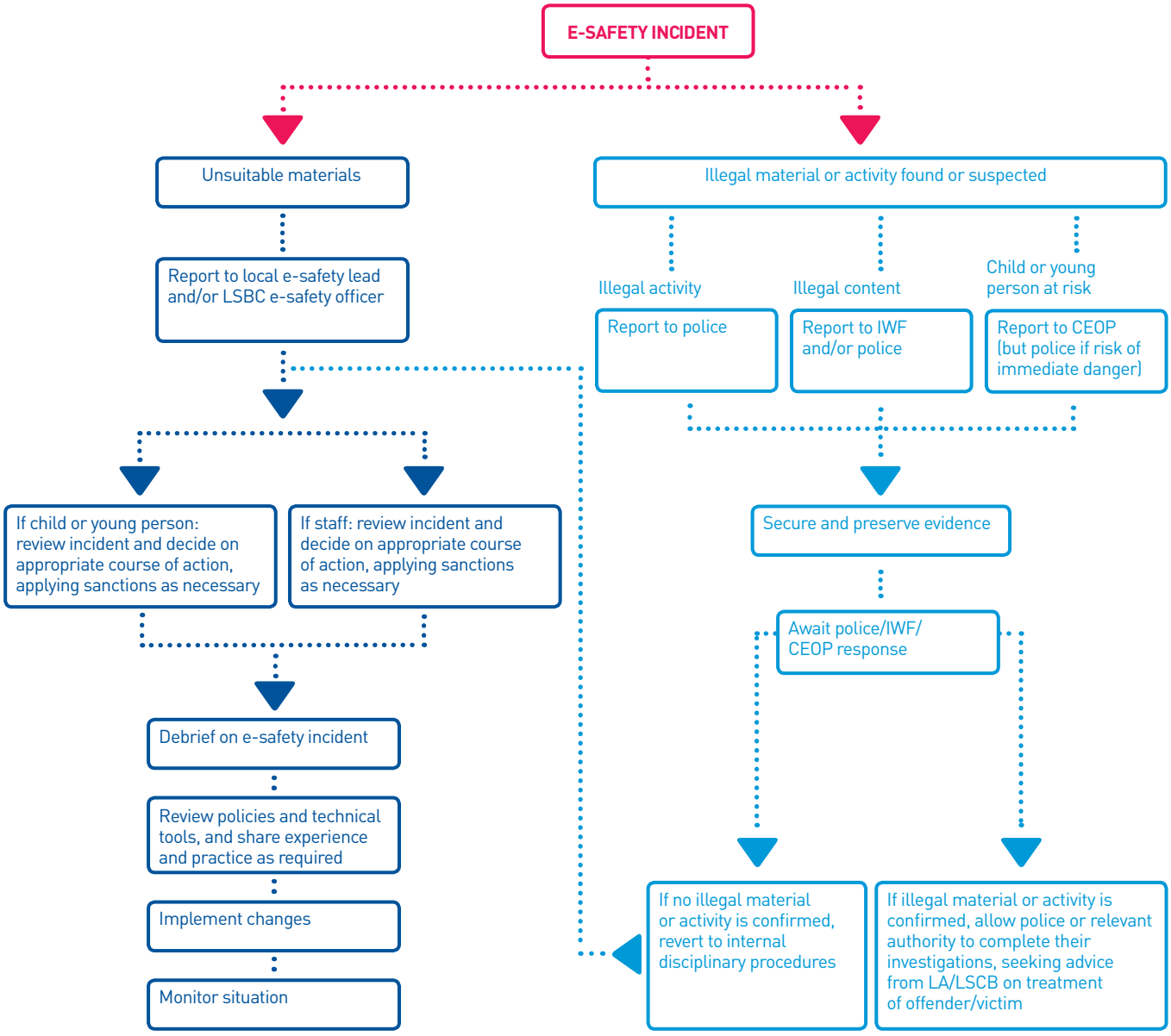
In earlier e-safety publications Becta has modelled an outline flowchart for responding to e-safety incidents in schools. We reproduce this opposite.

A key requirement in responding to e-safety incidents is to recognise when to escalate incidents. This involves recognising when to involve other agencies (such as child protection experts, social care, the police, the Internet Watch Foundation, or the Child Exploitation and Online Protection Centre) and securing and preserving evidence correctly.

In particular, schools must be aware of the local procedures to follow should e-safety incidents arise, including how and when to contact external agencies. Becta has been working with LSCBs to help them develop policies in this area. Schools and other children's services should seek to familiarise themselves with their LSCB policies and practice, and align their own policies and practice accordingly.

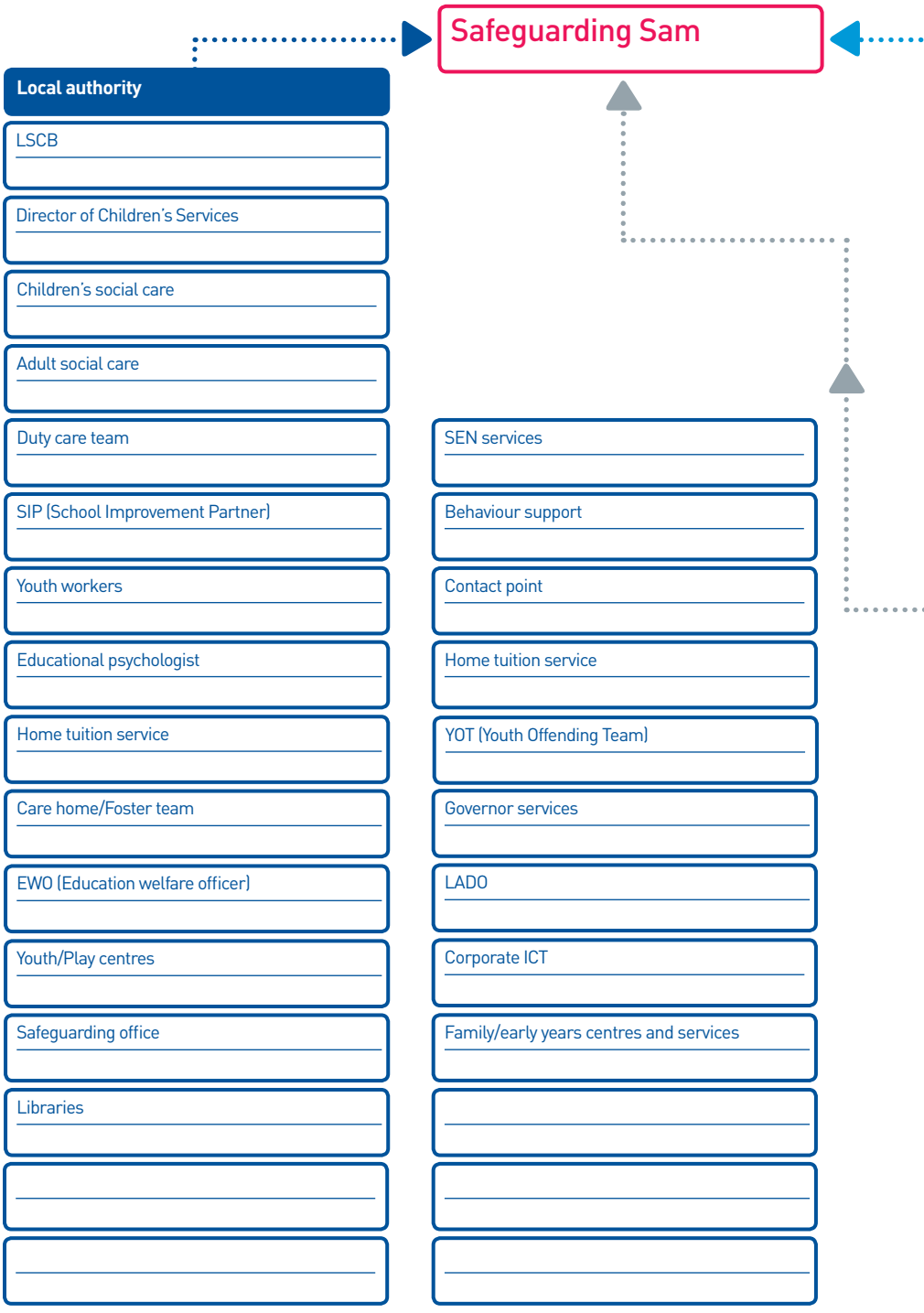
[28] www.becta.org.uk/nextgenerationlearningcharter

## Flowchart for responding to e-safety incidents



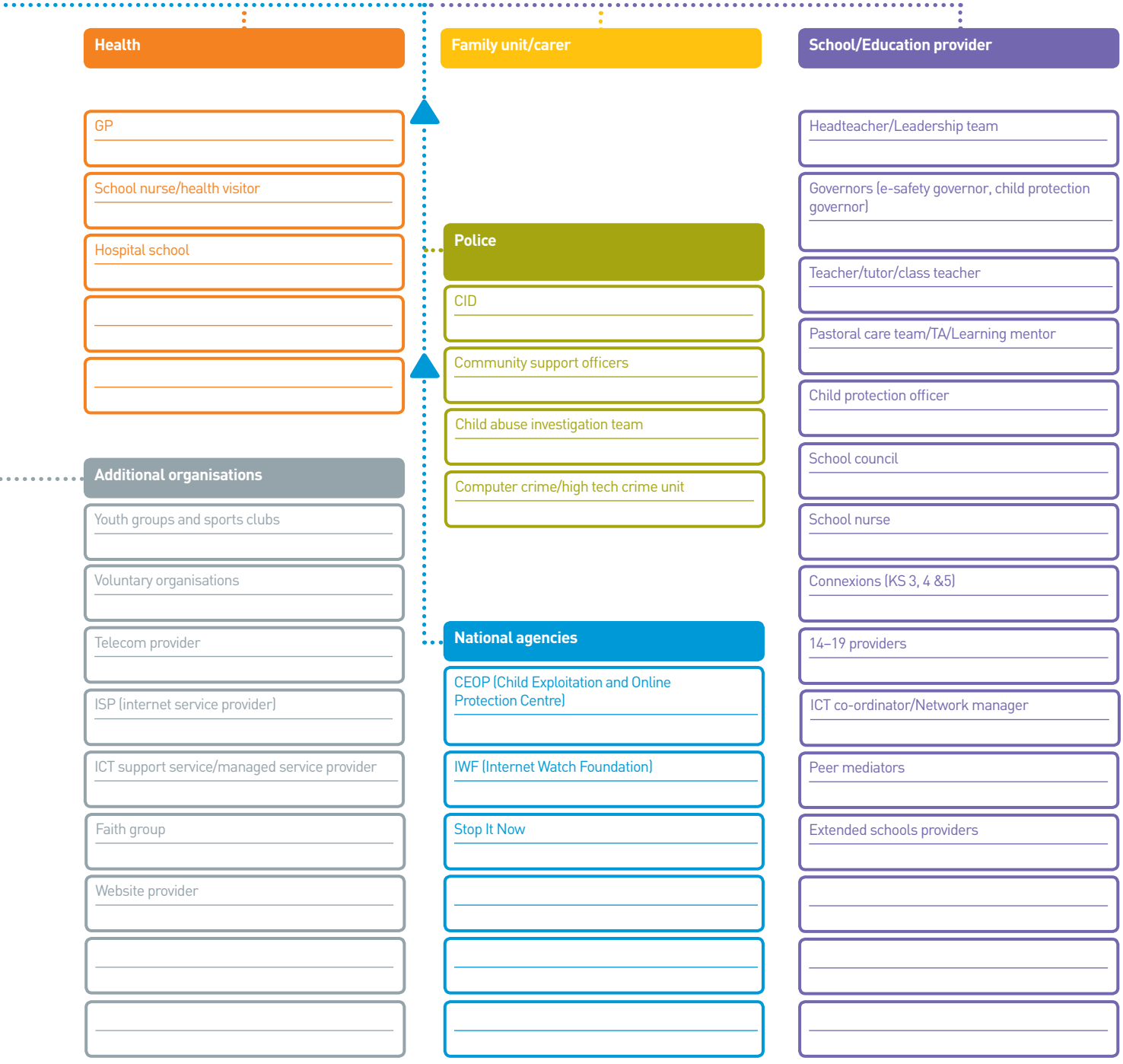
## Annex C: Safeguarding Sam mapping resource

In our LSCB toolkit, we provided a mapping resource, 'Safeguarding Sam'. The resource was intended to help LSCBs to document all the points of contact which might be needed when responding to an e-safety incident for any particular child. This is replicated below.




Where possible list contacts for 24/7/365

Schools, and other children's services, may wish to consider a similar approach for identifying, and recording their own local points of contact and support networks.



## Annex D: Acknowledgements

Becta would like to thank the following agencies and organisations for their involvement in this publication:

ADCS: The Association of Directors of Children's Services
www.adcs.org.uk

ASCL: Association of School and College Leaders
www.ascl.org.uk

ATL: Association of Teachers and Lecturers
www.atl.org.uk

CEOP: Child Exploitation and Online Protection Centre
www.ceop.gov.uk

ChildLine
www.childline.org.uk

Childnet International
www.childnet.com

DCSF: Department for Children, Schools and Families
www.dcsf.gov.uk

Deafax
www.deafax.org

European Schoolnet (EUN)
www.eun.org

IWF: Internet Watch Foundation
www.iwf.org.uk

Naace
www.naace.co.uk

NAHT: The National Association of Head Teachers
www.naht.org.uk

NASUWT: The National Association of Schoolmasters
Union of Women Teachers
www.nasuwt.org.uk

NCPTA: National Confederation of Parent Teacher Associations
www.ncpta.org.uk

NCSL: National College for School Leadership
www.ncsl.org.uk

National Strategies
www.standards.dcsf.gov.uk/nationalstrategies

NUT: National Union of Teachers
www.teachers.org.uk

Ofsted
www.ofsted.gov.uk

SSAT: Specialist Schools and Academies Trust
www.specialistschools.org.uk

Teachtoday
www.teachtoday.eu

Becta would also like to thank the following organisations for their contributions to the Becta e-safety working days in September 2008, and for their continued support in the writing and production of this and other Becta e-safety resources.

- Birmingham City Council
- Birmingham East City Learning Centre
- Bristol CLC3 (City Learning Centre)
- Cambridgeshire County Council
- Cornwall County Council
- Cumbria and Lancashire Education Online (CLEO)
- Derby City Council
- Dudley Metropolitan Borough Council
- European Schoolnet (EUN)
- Hertfordshire County Council
- Joint Information Systems Committee (JISC)
- Kent County Council
- Lancashire County Council
- Leeds City Council
- London Borough of Islington Council
- Northamptonshire County Council
- Northern Grid for Learning

- Nottingham City Council
- Oxfordshire County Council
- Royal Borough of Kensington and Chelsea
- Shropshire County Council
- Somerset County Council
- South West Grid for Learning (SWGfL)
- Staffordshire County Council
- Stoke-on-Trent City Council
- Suffolk County Council
- Tameside Metropolitan Borough Council
- Telford & Wrekin Council
- Warwickshire County Council
- West Berkshire Council
- West Midlands Regional Broadband Consortium (WMnet)
- Wolverhampton City Council
- Worcestershire County Council

And members of the:

- Becta Inclusion and E-safety Expert Reference Group
- Becta LSCB Expert Reference Group
- NEN Safeguarding Group
- Safeguarding FE & Skills Learners in a Digital World Working Group

Becta leading next generation learning



Additional photography reproduced by kind permission of the Department for Children, Schools and Families.

Millburn Hill Road
Science Park
Coventry CV4 7JJ

Tel: 0800 877 8777
Fax: 024 7641 1418
E-mail: customerservices@becta.org.uk

www.becta.org.uk

02/08-09/TWP0013/TT20289/15648/20k