Becta leading next generation learning

Safeguarding children in a digital world

Developing an LSCB e-safety strategy

Becta leading next generation learning

Safeguarding children in a digital world

Developing an LSCB e-safety strategy

Contents

Foreword

I am delighted to launch this e-safety strategy toolkit on behalf of Becta, to coincide with our second conference – Safeguarding Children in a Digital World. We all have a responsibility to safeguard and promote the welfare of children, and that responsibility must apply to the online world which is such an important part of the everyday life of children and young people.

New technologies open up many exciting benefits and opportunities for children and young people but they can also present some risks. Technology is becoming all pervasive, touching all areas of society, with children and young people having increasing access to personal technology such as web-enabled phones. We must ensure, therefore, that a framework is in place to help children and young people stay safe when using new technology, and to ensure that where problems do occur, children and young people (and their parents and carers) have support in dealing with them effectively.

Local safeguarding children boards (LSCBs) have a key role to play in this process. LSCBs must co-ordinate and ensure the effectiveness of what their member organisations do both individually and together to safeguard and promote the welfare of children. This document outlines how LSCBs, and their member organisations, can set priorities and put in place action plans to ensure that they are contributing effectively to e-safety.

I commend the guidance given in this document to all LSCBs. It is only through a combined and consistent approach to e-safety that we can ensure that all children and young people are safeguarded from harm, wherever and whenever they go online.

Stephen Crowne

Chief Executive

Introduction

Since 1998, in conjunction with the Department for Children, Schools and Families (DCSF) (and its previous incarnations), Becta has been providing advice and guidance to schools and local authorities (LAs) on all aspects of e-safety.

Recognising that e-safety is not just the responsibility of educational practitioners, Becta has increasingly promoted the importance of a combined approach to policy, infrastructure and education, underpinned by inspection and standards, in helping to create a safe online environment for children and young people, wherever and whenever they go online. Some of Becta's previous publications have referred to this as the PIES model – see **Figure 1** below.

Recent years have seen the emergence of a wider strategic context into which e-safety falls, mainly embedded within safeguarding strategies. *The Children Act 2004*[1] provides the main legislative framework for wider strategies for improving children's lives, with the overall aim of encouraging integrated planning, commissioning and delivery of services to children, and for improving multidisciplinary working. This act provided the legal underpinning to *Every child matters: Change for children*[2] which focuses on five key outcomes for every child and young person, including the requirement to 'stay safe'. Recent government research activities such as the *Staying safe consultation*[3] and the *Byron review of children and new technology*[4] have promoted further the importance of e-safety.

Local safeguarding children boards (LSCBs) were formed in 2006, with a particular focus on aspects of the 'staying safe' outcome of *Every child matters*. They are the 'key statutory mechanism for agreeing how relevant organisations in each area will co-operate to safeguard and promote the welfare of children in that locality, and for ensuring the effectiveness of what they do'[5]. E-safety must therefore be part of their remit.

Becta quickly recognised the need to engage with LSCBs. Following the inaugural Safeguarding Children in a Digital World Conference in February 2006, Becta produced a series of practical checklists for LAs and LSCBs in a publication titled *Safeguarding children online: a guide for local authorities and local safeguarding children boards*[6].

Becta's work in this area has continued since then, with representatives from LAs and LSCBs meeting together in a series of working days in September 2007 to discuss models of best practice for developing a core LSCB e-safety strategy (see **Acknowledgements** for a list of participating LAs).

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

2 See Every Child Matters website [**http://www.everychildmatters.gov.uk**].

3 See Every Child Matters website [**http://www.everychildmatters.gov.uk/stayingsafe**].

4 See Byron Review website [**http://www.dfes.gov.uk/byronreview**].

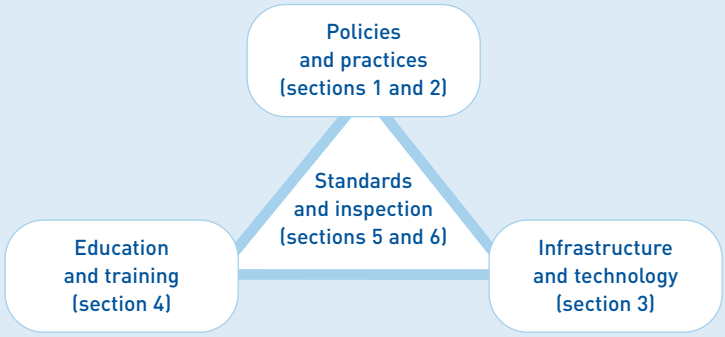
5 See paragraph 3.2 of *Working together to safeguard children: A guide to interagency working to safeguard and promote the welfare of children*, available on the Every Child Matters website [**http://www.everychildmatters.gov.uk/workingtogether**].

6 See Becta publications website [**http://publications.becta.org.uk/display.cfm?resID=31051**].

This document, published to coincide with the second Safeguarding Children in a Digital World Conference in February 2008, is the output of those working days.

Specifically, it aims to drive the e-safety agenda forward for LSCBs, offering a framework for a national standard of best practice that boards may adopt and adapt locally to meet local safeguarding needs and conditions.

Figure 1:
PIES model for limiting e-safety risks



The content of this document broadly maps to the PIES model, as illustrated in **Figure 1**.

This document does not intend to prescribe a 'one-size-fits-all' approach, but instead offers a set of core prompts and some sample materials to help LSCBs in developing their own strategies, systems and processes which will ultimately help children stay safe in the digital world. It does not set out requirements for LSCBs: rather it aims to provide useful principles and examples which LSCBs can draw on.

We recognise that the work of LSCBs is still developing, with a recent review of progress[7] stating: '...LSCBs need to ensure they continue to evaluate their own progress, identify the challenges they still face, and commit to actions necessary to overcome these challenges and improve performance' if they are to realise their full potential. Equally, LSCB approaches to e-safety will develop and mature over the coming years, and Becta will continue to support them in their work.

Please note that we do not intend to update this document in print. While it offers a starting point for developing an LSCB e-safety strategy, we hope that LSCBs and their member agencies will rapidly move beyond the stages outlined here. Becta's work will therefore concentrate on supporting LSCBs in their continuing e-safety work once they have established a strategy. Hard copies of this document will not be available beyond its initial circulation, but you will be able to download electronic copies from the Becta website[8].

To keep up to date with the latest e-safety information, LSCBs, member agencies and others with an interest in Becta's e-safety work may like to join the Safetynet mailing list – see **Section 8** below for further information.

[7] See Ministerial Foreword of *Local safeguarding children boards: A review of progress*, available on the Every Child Matters website [**http://www.everychildmatters.gov.uk/lscb**].

[8] See Becta website (**http://www.becta.org.uk/localauthorities**).

Definition of key terms and concepts

In this document, as in the *Children Act 1989*[9] and the *Children Act 2004*[10] (and various safeguarding guidance), a child is defined as anyone who has not yet reached their eighteenth birthday. Where we use the word 'child' (or its derivatives) in this document, we mean 'child or young person'.

Terms such as 'e-safety', 'online', 'communication technologies' and 'digital technologies', when used in this document, refer to all fixed and mobile technologies that children may encounter, now and in the future, which allow them access to content and communications that could raise e-safety issues or pose risks to their wellbeing and safety.

The term 'safeguarding' is defined for the purposes of this document in relation to e-safety as the process of limiting risks to children when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection.

Working together to safeguard children[11] uses the following terms:

- 'Board partner' means statutory organisations that are required to co-operate in the establishment and operation of the LSCB (paragraph 3.58)
- 'Other members' means other relevant local organisations which should be involved in the work of the LSCB (paragraph 3.62)
- 'Other agencies and groups' refers to organisations and individuals that may be involved in LSCB work on an 'as needed' basis (paragraph 3.63)
- 'Key national organisations' refers to organisations such as CEOP that are involved in the wider safeguarding agenda (paragraph 3.64).

Where appropriate, this document follows the same conventions, but also uses the wider term 'member agencies' to mean all of those organisations, from any of these groupings, which may be involved in LSCB e-safety strategy work.

[9] See Children Act 1989 [**http://www.opsi.gov.uk/acts/acts1989/Ukpga_19890041_en_1.htm**].

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

[11] See Working together to safeguard children [**http://www.everychildmatters.gov.uk/workingtogether**].

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 multifaceted and, as case law in this area is still very much under development, nothing in this publication constitutes legal advice.

If you have a specific query, you should seek advice from appropriate advisors, who may include your local authority children's services, child protection experts, the police, the Child Exploitation and Online Protection (CEOP) Centre, Internet Watch Foundation (IWF), counsellors, legal advisers, the DCSF and 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 publication were correct at the time of publication, but may be subject to change over time.

Becta leading next generation learning

Contents

Developing an LSCB e-safety strategy

Becta leading next generation learning

1

Developing an e-safety strategy

Why develop an e-safety strategy?

Aims and objectives of an e-safety strategy

Embedding the e-safety strategy in the wider work of the LSCB

Developing an e-safety strategy

Why develop an e-safety strategy?

LSCBs have a statutory duty to safeguard and promote the welfare of children in their locality and, as technology increasingly permeates into every aspect of a child's life from an ever-younger age, e-safety must necessarily be part of this remit.

Often referred to as 'digital natives'[12], children are now citizens born into a digital world, growing up surrounded by and immersed in the technology and tools of the digital age. Children's access to technology has increased phenomenally in recent years: ICT is embedded in reception classrooms and is a constant and prevalent feature of school life; home access is on the increase, while connectivity from public locations such as libraries and youth clubs is now commonplace. Equally, the convergence of technologies and decreasing costs of ownership mean that, with access to a whole range of online services from mobile phones to games consoles and similar devices, children are no longer restricted to accessing the internet from a fixed location.

While it is clear that technology offers children unprecedented opportunities to learn, communicate, create, discover and be entertained in a virtual environment, there are some inherent risks. And while most children's confidence and competence in using the technologies is high, their knowledge and understanding of the risks may be low.

E-safety risks have traditionally been classified as those involving content, contact and commerce. When online, for example, children may be exposed to inappropriate content which may upset or embarrass them, or which could potentially lead to their involvement in crime and anti-social behaviour. Some people use the internet to groom children with the ultimate aim of exploiting them sexually, while ICT offers new weapons for bullies who may torment their victims, for instance using websites or text messages. The recent surge in popularity of self-publishing and social networking sites brings new e-safety challenges, with many young people making available online some detailed – and sometimes inappropriate – personal information, which again raises both content and contact issues. And while the internet offers new opportunities for doing business online, it also brings with it many unscrupulous traders to whom children and young people may be particularly vulnerable. Previous Becta e-safety publications have discussed these issues and risks in depth (see **Section 8** for further details).

Children need guidance in developing their own set of responsible behaviours to keep them safe when online, but equally they should know that, if things go wrong, they may seek help and support from any trusted adult. Consideration should also be given to supporting children with special educational needs (SEN), who may require additional support and guidance in the online world.

[12] Prensky, M (2001), 'Digital natives, digital immigrants' in *On the horizon* 9(5), October, NCM University Press [**http://www.marcprensky.com/writing/Prensky - Digital Natives, Digital Immigrants - Part1.pdf**].

All agencies providing services to children have a duty to understand e-safety issues, recognising their role in helping children to remain safe online while also supporting adults who care for children.

The emphasis should be very much on how to use digital technologies safely and responsibly, rather than on a blocking and banning approach.

It must be recognised that e-safety is not a technological issue and is not limited to settings where children have access to technology. Likewise, responsibility for e-safety must not be delegated to technical colleagues or those with a responsibility for ICT, but must be firmly embedded within safeguarding policies, practices and responsibilities.

Although agencies that do provide online access have a duty to ensure that their technological infrastructure is safe and secure, filtered and monitored, and that appropriate acceptable-use policies are in place (see also **Section 3** below), e-safety responsibilities extend much further.

All agency staff who have contact with children should promote the safe and responsible use of technology in its many forms. They should learn to recognise the behaviours in children that may indicate that they are at risk from e-safety issues, and know where to go for further help. Equally, all staff should be aware of the appropriate response if a child directly divulges an e-safety incident, how to assess the safeguarding implications and how to escalate it appropriately.

The role of the LSCB is to co-ordinate and ensure the effectiveness of e-safety work across all member agencies, and the development of an LSCB e-safety strategy will help in this process.

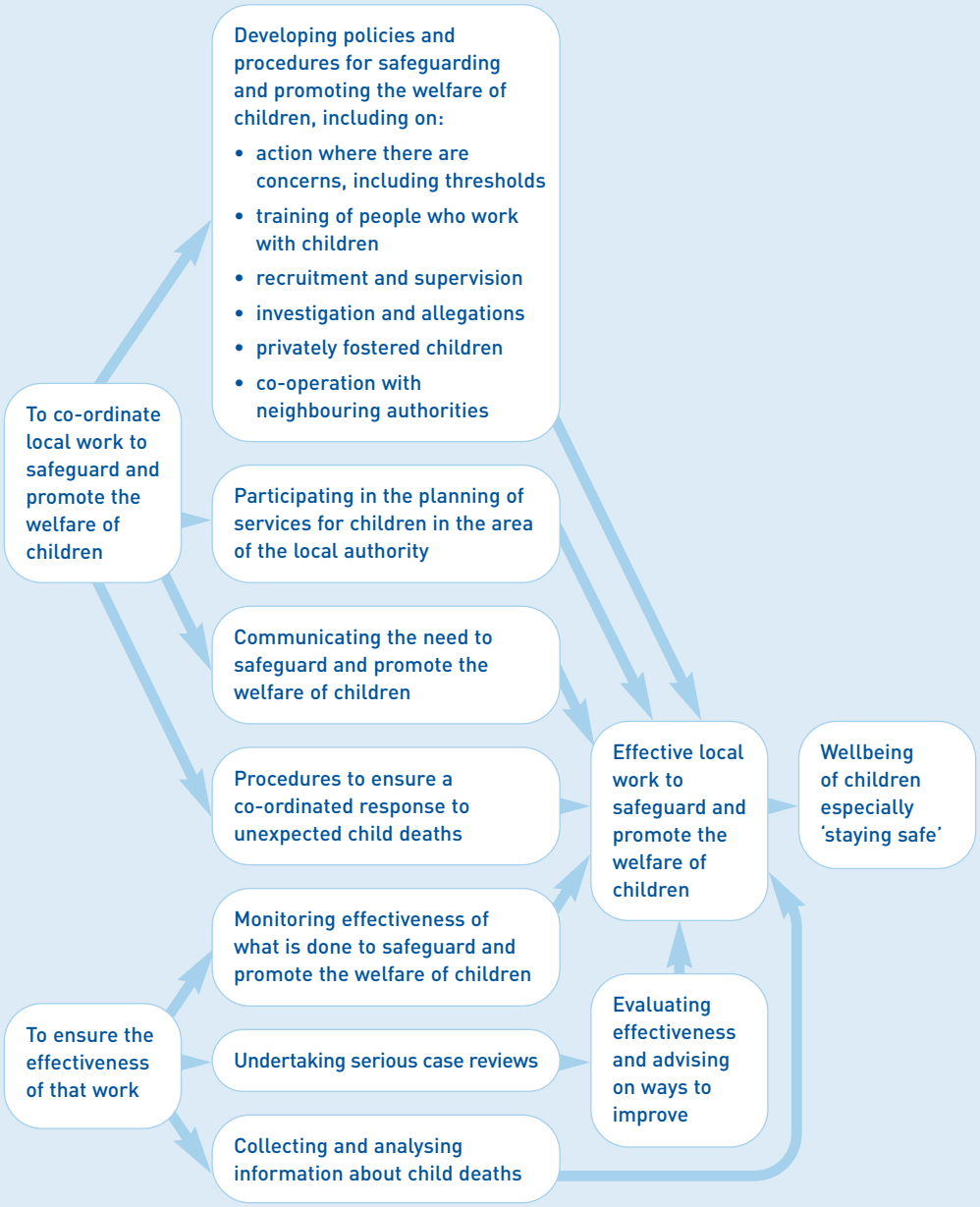
Aims and objectives of an e-safety strategy

LSCBs should develop a set of aims and objectives to define their e-safety responsibilities. These might include the following:

- Recognising the importance of e-safety within the context of *Every child matters*
- Recognising the importance of e-safety within the wider work of the LSCB
- Recognising that e-safety is not a technological issue
- Recognising the importance of education, training and information
- Recognising the need to monitor the impact of the strategy.

If we consider the wider context within which LSCBs operate, Chapter 3 of *Working together to safeguard children* sets out the core LSCB objectives and functions, presenting these diagrammatically as reproduced in **Figure 2**.

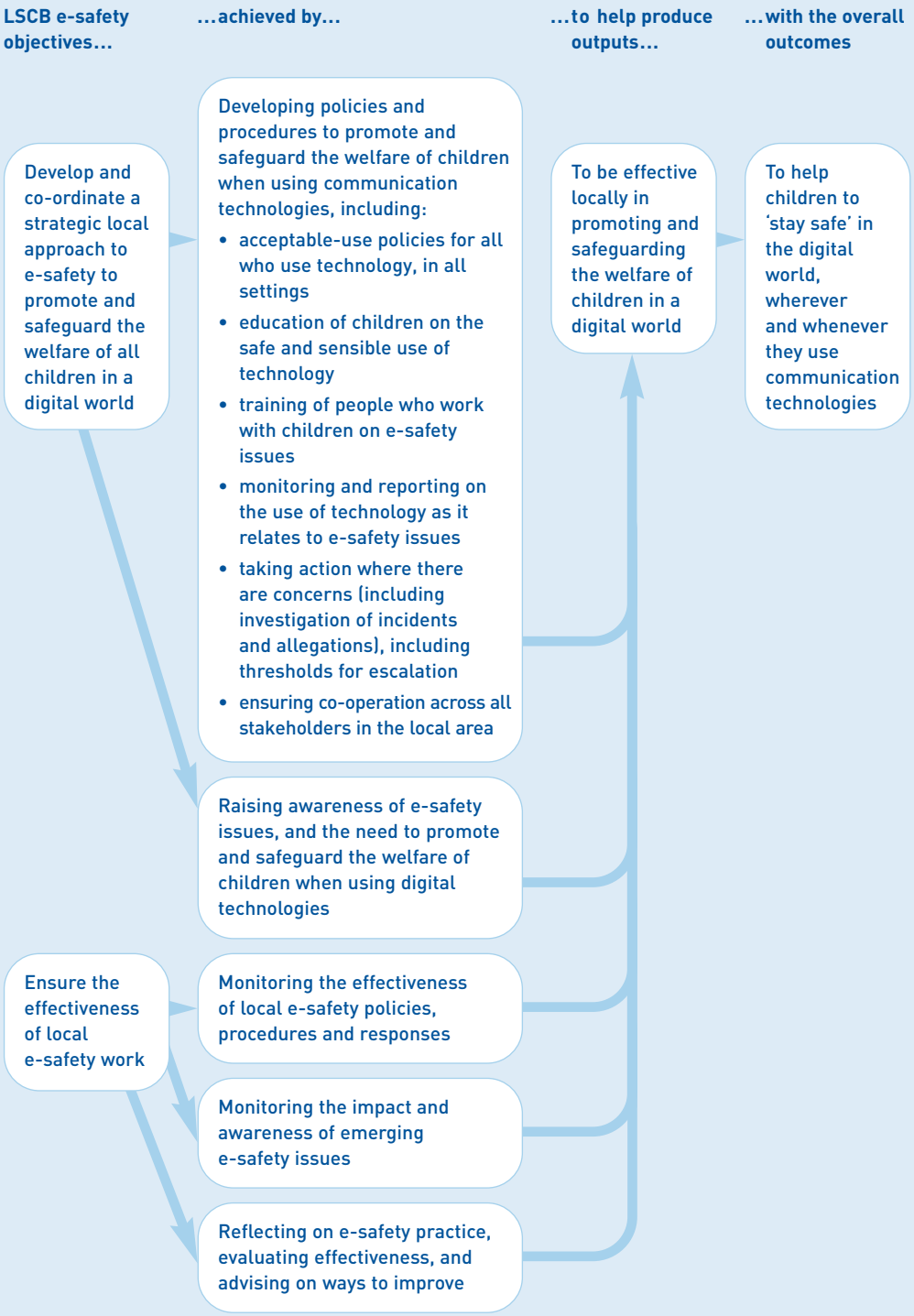
Figure 2:
LSCB objectives and functions



(Reproduced from *Working together to safeguard children*, Chapter 3, page 75, Figure 1)

If we consider how e-safety can contribute to this overall framework, we can broadly define the LSCB e-safety objectives and functions as shown in **Figure 3**.

Figure 3:
Proposed model for LSCB e-safety objectives and functions



Each LSCB must consider e-safety issues within its local context and develop its e-safety strategy accordingly.

Equally, when developing a strategy, LSCBs must recognise that their role in e-safety is a strategic rather than operational one. As discussed in *Working together to safeguard children* (paragraph 3.16):

> '...while the LSCB has a role in co-ordinating and ensuring the effectiveness of local individuals' and organisations' work to safeguard and promote the welfare of children, it is not accountable for their operational work. All Board partners retain their own existing lines of accountability for safeguarding and promoting the welfare of children by their services. The LSCB does not have a power to direct other organisations.'

The same must necessarily be true of any e-safety work within a given locality.

LSCBs should seek to evaluate the effectiveness of their e-safety work through a peer-review process, based on self-evaluation, performance indicators and joint audit. During the creation of their e-safety strategy, therefore, LSCBs must give consideration to how to conduct the process. Equally, there must be synergy between the evaluation of e-safety work and the core LSCB monitoring and evaluation role. It is important to consider how these two areas of work can support each other.

Individual children's services continue to be assessed through their own quality and inspection regimes, and the LSCB should consider how it can feed into this process with respect to e-safety issues.

E-safety in practice – key objectives

Dudley Safeguarding Children Board (DSCB) has established an e-safety strategy with the following key objectives:

- Ensuring that all children, young people and parents/carers are equipped with the knowledge and skills to safeguard themselves online
- Ensuring that all children who have been the subject of indecent images and sexual exploitation are identified, protected and given an appropriate level of support
- Ensuring that all people who work with children and young people have access to good quality procedures and effective training to safeguard children at risk through online activity
- Ensuring that systems and services are in place to identify, intervene and divert people from sexually exploiting or abusing children online and offline.

Thanks to Dudley Metropolitan Borough Council for sharing this material

Embedding the e-safety strategy in the wider work of the LSCB

To be effective, the e-safety strategy must be rooted in the wider work of the LSCB. It must be firmly embedded in the business planning process to ensure appropriate resourcing and funding, and aligned with the work of LSCB committees and subgroups to ensure maximum impact in the local area.

For further case study materials outlining how various LSCBs have approached e-safety, see Annex A.

Becta leading next generation learning

2

Developing an e-safety subgroup

Why develop an e-safety subgroup?

Ownership of the e-safety subgroup

Membership of the e-safety subgroup

Terms of reference

Roles, responsibilities and accountabilities

Programme of work

Resourcing

Communication and awareness raising

Developing an e-safety subgroup

Why develop an e-safety subgroup?

Guidance given in *Working together to safeguard children* (paragraph 3.68) states that it may be appropriate for LSCBs to set up working groups or subgroups to carry out specific tasks or provide specialist advice. This may be, for example, either on a short-term or standing basis to carry out specific tasks, provide specialist advice, bring together representatives of a sector to discuss relevant issues, or focus on defined geographical areas within the LSCB's boundaries.

Becta therefore recommends that LSCBs convene a standing e-safety subgroup to drive forward the e-safety strategy and to give a real focus and momentum to this important area of work.

Ownership of the e-safety subgroup

There must be clear ownership of the e-safety subgroup.

In line with general guidance on subgroups (*Working together to safeguard children*, paragraph 3.71), the e-safety subgroup should be chaired by an LSCB member to ensure cohesion and continuity with the wider work of the LSCB.

The e-safety subgroup should work to agreed terms of reference, which should define its remit, explicit lines of reporting, communication and accountability. All LSCBs should develop generic job descriptions for subgroup members.

Membership of the e-safety subgroup

The membership of the subgroup must be clearly defined and should include:

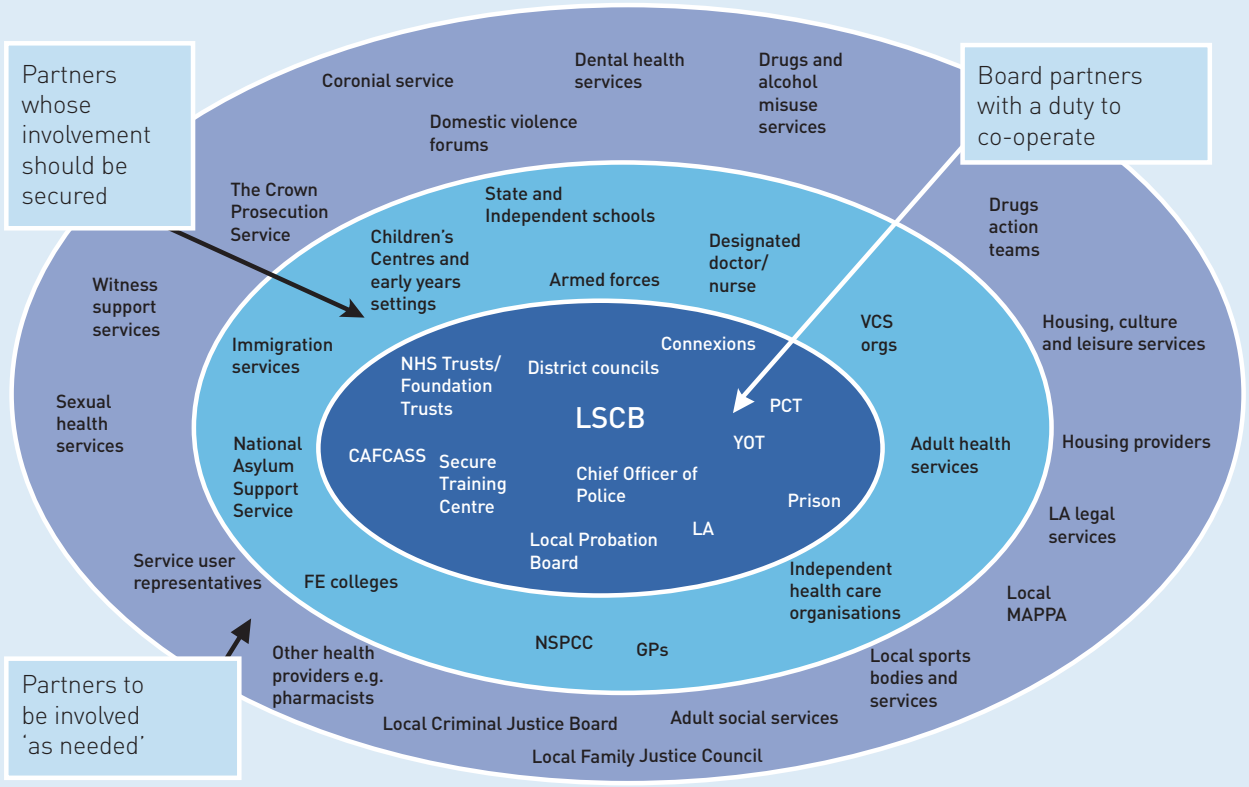
- identification of the subgroup chair (who should be a member of the LSCB, as discussed above)
- core/mandatory representation
- co-opted representation as needed.

It may be necessary for membership to change over time as the role and remit of the group develops and matures. However, it is recommended that the core representation within the group be reasonably small so that the group can remain focused and on task, and can progress essential issues with speed and efficiency.

The document *Local safeguarding children boards: A review of progress*[13] contains a graphical model for LSCB membership, as reproduced overleaf:

[13] See *Local safeguarding children boards: A review of progress*, available on the Every Child Matters website [**http://www.everychildmatters.gov.uk/lscb**].

Figure 4:
LSCB membership



(Reproduced from *Local safeguarding children boards: A review of progress*, Background to the priority review, page 11, Figure 2)

A similar approach may be useful for modelling the membership of the e-safety subgroup. Such an approach will also be useful for identifying agencies or stakeholders that may be on the periphery of e-safety activity, but that LSCBs would still need to include in their e-safety communications plan (see below).

E-safety in practice – subgroup membership

Brent LSCB has taken a strategic and considered approach to e-safety. The following extract, taken from a longer case study (see **Annex A**), outlines the Brent approach to defining its e-safety subgroup membership.

'When working out whom to invite to join the group we started by considering access points: access points to the internet and access points to children and young people. Which agencies were providing internet access to children and young people? Which agencies would give us access to children and young people for education campaigns or research?

Our initial membership therefore was:

- Head of Systems and Performance Management (Children and Families Department)
- Principal Information Officer (Social Care)
- London Grid for Learning (Regional Broadband Consortium)
- Education Child Protection Advisor (Children and Families Department)
- IT Security Manager (LA Corporate IT)
- Detective Inspector, Child Abuse Investigation Command (Metropolitan Police).

The group has since expanded to include representation from City Learning Centres, the Primary Care Trust, the School Improvement Service, the Extended Schools Programme and Arts and Libraries.

Based on our experience, our main recommendation would be to get your group membership right and think laterally about whom it should include. Expect and accept that by necessity the membership could change.'

Thanks to colleagues at Brent for sharing this material

Terms of reference

The e-safety subgroup must develop clear terms of reference, linked to the wider LSCB terms of reference. These might include:

- The key strategy aspects of the subgroup, which might cover:
  - communication and awareness raising
  - education and training
  - monitoring and reporting
  - responding to specific incidents
- Relationships with other LSCB committees and subgroups, including clear reporting lines in both directions
- Relationships with other key stakeholders, including internal agencies, external 'expert' agencies (such as CEOP and Becta) and other organisations.

E-safety in practice – developing terms of reference

Knowsley Safeguarding Children Board (KSCB) has embedded e-safety in its business planning, convening the Safer Internet Task Group with the following terms of reference:

- To develop a strategy for a pan-Knowsley approach to promoting the safer use of ICT
- To work in partnership to address specific areas of concern, particularly where children and young people may be at risk of harm
- To co-ordinate awareness-raising training for staff, parents, carers, children and young people
- To provide advice and support to colleagues and the community on safeguarding aspects of the use of ICT.

Through the business plan, the work of the Safer Internet Task Group is firmly embedded in other subgroups. These include the Policy and Procedure Group (for producing policy and guidance), the Safer Workforce Development Group (for ensuring that staff receive relevant training on e-safety issues) and the Performance and Scrutiny Group (to ensure that incidents are properly reported and action is taken).

Thanks to colleagues at Knowsley Metropolitan Borough Council for sharing this material

Roles, responsibilities and accountabilities

After agreeing the terms of reference of the e-safety subgroup, LSCBs must define clearly its roles, responsibilities and accountabilities, and also set a schedule of meetings and a timetable for reporting progress. These may be linked to the programme of work (see below).

Additionally, LSCBs need to outline the co-operation which will be required between various agencies, along with an indication of the boundaries of their respective responsibilities, particularly if responding to specific e-safety incidents.

Programme of work

The e-safety subgroup should develop a programme of work against which its outputs and effectiveness can be monitored and reviewed.

A good starting point might be to audit what already exists locally in relation to the PIES model, identify existing good practice and expertise, and set priorities for future effort. We give some examples below.

- Policies and practices

  What policies and practices already exist in each of the member agencies? Is there a designated officer with responsibility for e-safety in all member

agencies? Is there a forum in which agencies may liaise and communicate? Are there any models of good practice which could be developed and shared across the locality? Are there any gaps and, if so, how should these be prioritised?

In the first instance LSCBs may wish to draw on the expertise of schools in their area. Many schools, with the support of local regional broadband consortia (RBCs), may already be quite mature in this area and thus able to share experiences and expertise with other children's services.

- Infrastructure and technology

  What are the infrastructure and technology issues in the locality? Are minimum infrastructure standards in place in each setting? What infrastructure policies and practices already exist in each of the member agencies? Are there any models of good practice which could be developed and shared across the locality? Are there any gaps or infrastructure vulnerabilities and, if so, how should these be prioritised?

  Again, LSCBs may like to start by drawing on the expertise of schools and RBCs.

  For more on infrastructure issues see **Section 3** below.

- Education and training

  What expertise, education and training already exist across the member agencies? Are there any gaps in knowledge and, if so, how should these be prioritised and addressed? Can education and training needs be differentiated across the various member agencies, and across different stakeholder groups? How will education and training be facilitated? And how will its effectiveness be evaluated? Which external organisations can help with education and training?

  We discuss education and training further in **Section 4**.

- Standards and inspection

  What standards and inspection regimes already exist across the member agencies, and how might these contribute to the e-safety strategy? What should member agencies monitor and report on? What does the LSCB wish to monitor and report on? How will the process be managed and co-ordinated?

  Standards and inspection issues are discussed further in **Section 5**.

From this, e-safety subgroups may develop a detailed and prioritised programme of work which should include clear, accountable actions and a timeline for achieving key milestones.

The programme of work – which LSCBs should review, monitor and refine regularly as the e-safety strategy matures – will form a major aspect of the evidence of effectiveness.

An exemplar LSCB e-safety strategy and action plan appears at Annex G.

Resourcing

The e-safety subgroup must consider resourcing issues, both in terms of the personnel and budget needed to deliver the specific objectives of the e-safety strategy, and in terms of other resource and support needed from across the wider LSCB. Subgroups must therefore ensure that e-safety is embedded within the wider LSCB business planning process.

Communication and awareness raising

Communication and awareness raising is a key aspect of the e-safety strategy, and should be a two-way process between the LSCB and all stakeholder groups. The e-safety subgroup should consider developing an e-safety communications plan as a priority action, working with the wider LSCB communications committee or subgroup as appropriate.

It may be useful to consider such a plan in terms of several key elements.

- Communication with member agencies

  The e-safety subgroup should consider how it will communicate with all member agencies. Regular and ongoing contact with member agencies will be essential in raising awareness of e-safety issues, and in helping those agencies to recognise the importance of their role in safeguarding children in a digital world.

- Communication with children, parents and carers

  As advised in paragraph 3.73 of *Working together to safeguard children*, LSCBs should consider how they can engage with these stakeholder groups, and this may help to identify local e-safety priorities:

  'LSCBs should consider how to put in place arrangements to ascertain the views of parents and carers and the wishes and feelings of children (including children who might not ordinarily be heard) about the priorities and effectiveness of local safeguarding work, including issues of access to services and contact points for children to safeguard and promote welfare. LSCBs should also consider how children, parents and carers can be given a measure of choice and control in the development of services.'

  Regular and ongoing contact with children, and their parents and carers, can help to reinforce key e-safety messages, increase awareness and generally promote a shared responsibility in e-safety, thus increasing the effectiveness of local education and training strategies.

  The e-safety subgroup should identify opportunities for communicating with these stakeholder groups and for soliciting feedback from them. The Youth Parliament, for example, might be one route to gathering the views of young people, while the local parenting strategy (a requirement for all local authorities by March 2008[14]) might be a further useful channel.

[14] See Parenting support information on the Every Child Matters website [**http://www.everychildmatters.gov.uk/resources-and-practice/IG00169**].

- Communicating with the media

  The media can play an important role in promoting e-safety awareness, so the e-safety subgroup should consider how it can engage effectively with the local press.

  The media are often quick to pick up on stories with a negative e-safety aspect, but they also have a responsibility for promoting information on positive uses of digital technologies and the good practice messages that go alongside this. Some LSCBs have secured media representation in their e-safety subgroup to very good effect.

E-safety in practice – working with the media (1)

Solihull Metropolitan Borough Council has developed an extensive guide on working with the media.

Specifically aimed at the education sector, the guide is designed to help schools to capture good news stories, to deal with enquiries from both the print and broadcast media, and to know how to respond if an emergency occurs. It explains how schools can help themselves by being prepared, knowing the rules of the game and being clear about what makes a good news story. It also explains how the Council's press office supports schools in this process.

LSCBs may wish to consider developing a media plan such as this as an aspect of their e-safety strategy. All member agencies should take a role in sharing positive e-safety stories with the media, but equally should know how to deal with the press should an e-safety incident or emergency occur.

Thanks to colleagues at Solihull Metropolitan Borough Council for sharing this material

E-safety in practice – working with the media (2)

Telford and Wrekin LSCB outlines its approach to working with the media:

In Telford and Wrekin, our LSCB e-safety subgroup took a conscious decision to foster better links with the press.

While the priority is safeguarding young people online, sometimes circumstances dictate that negative or sensational headlines are generated. We feel that some of these headlines are a reaction that comes from not fully understanding the risks and benefits of technology. By demonstrating through the local press that e-safety awareness is promoted and taught, this helps to generate public interest and awareness.

The local authority provides information and stories to the public relations department to enable them to give details when the press contact them for

stories. This strategy engages the press in a more constructive and proactive way. By this approach we hope that when there are highly dramatic headlines to be released, the press will already have information that allows them to be more balanced... or at least they will know whom they can contact with an opportunity to respond or present a balanced view.

Some tips for others who want to improve the way they communicate their efforts include:

- Always consider the target audience. You are unlikely to reach all demographic groups with the same story, so tailor your approach accordingly. Consider the group that you are trying to reach, and target the most appropriate media. Much effort will be wasted if the target audience is not clear.
- Create a public relations or communications plan. Set out how you intend to increase coverage and how to build links with the press.
- The LSCB should have a nominated person who is prepared to deal with enquiries from the press.
- Talk to the reporters who approach you regularly and find out what details they require in a press release. Write in the style of an article that a hard-pressed reporter could copy and paste. Supplement it with 'notes to editors' that include contact details for further information or to arrange an appointment for a photographer. Consider including a selection of quotes from key people to avoid reporters randomly approaching them for quotes that they may not be prepared for. Remember to fully brief the person you are quoting, and consider giving different versions of the same message.
- Keep a few non-time-critical press releases ready to release at short notice.

Thanks to colleagues in the Borough of Telford and Wrekin for sharing this material

Annex A has further case studies that illustrate how other LSCBs have approached e-safety.

Becta leading next generation learning

Developing an e-safe infrastructure

3

Why develop an e-safe infrastructure?

Identifying key stakeholders in infrastructure issues

Risk assessment

Use of accredited services

Developing filtering standards

Developing acceptable-use policies

Monitoring and reporting

Infrastructure staff

Responding to specific incidents

Legislative considerations

Developing an e-safe infrastructure

Why develop an e-safe infrastructure?

As already discussed in **Section 1**, infrastructure issues are just one aspect of an e-safety strategy but they are nonetheless vitally important. In technology-based services to children, a robust infrastructure can offer a first line of defence against e-safety risks, which must then supplemented by the policy, education and standards aspects of the PIES approach.

LSCBs, through their e-safety strategy, have a role to play in giving advice and guidance to member agencies on developing an e-safe infrastructure. Although LSCBs have no operational control over the services which come under their remit (as discussed in **Section 1**), the focus should be on developing a set of core infrastructure principles which all children's services should aspire to achieve.

Identifying key stakeholders in infrastructure issues

One of the first actions which the e-safety subgroup should undertake is to identify the local settings where infrastructure issues require consideration. For example, these might include the following:

- Schools
- Pupil referral units (PRUs) and EOTAS (education other than at school) services
- Post-16 and adult education providers (including colleges)
- Connexions (including work-based learning settings)
- City learning centres (CLCs)
- Libraries
- Youth clubs and youth groups
- Community centres
- Children in care (CiC)
- Children's homes
- Long-term sick
- Universal home access (including Computers for Children schemes)
- Children's centres
- Youth offending services
- Probation services
- Private ICT training centres
- Internet cafés
- Primary care trusts (PCTs)
- Acute trusts.

There may also be others, depending on the local context in which the LSCB operates, and new settings may emerge over time.

The 14–19 diploma, for example, will raise new cultural and technical challenges for e-safety with a duty to protect young people who may be learning in the workplace, as will the implementation of learning platforms, giving every learner access to a personalised online learning space. LSCBs should consider such developments in their planning.

A priority for the e-safety subgroup will be to engage all local services that work with children (including services in the third sector) in the e-safety debate. They should make them aware of the duty of care and accountability issues in delivering technology-based services to the local community, and seek to establish an e-safety contact or responsible officer within each service.

Although it is neither likely nor desirable to have representatives from each of these agencies to sit on the e-safety subgroup, they should form part of the communication plan, and may be co-opted onto the subgroup as needed.

LSCBs should also seek to identify other stakeholders, such as the local RBC, who may be able to offer further support in infrastructure issues.

E-safety in practice – the role of RBCs

RBCs – partners in the National Education Network – are consortia of local authorities established to procure cost-effective broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authority areas as follows:

- CLEO: Cumbria Lancashire Education Online [**http://www.cleo.net.uk**]
- EMBC: East Midlands Broadband Consortium [**http://www.embc.org.uk**]
- E2BN: East of England Broadband Network [**http://www.e2bn.org**]
- LGfL: London Grid for Learning [**http://www.lgfl.net**]
- NG: Northern Grid [**http://www.portal.northerngrid.org**]
- NWLG: North West Learning Grid [**http://www.nwlg.org**]
- SEGfL: South East Grid for Learning [**http://www.segfl.org.uk**]
- SWGfL: South West Grid for Learning [**http://www.swgfl.org.uk**]
- WMnet: West Midlands Regional Broadband Consortium [**http://www.wmnet.org.uk**]
- YHGfL: Yorkshire & Humberside Grid for Learning [**http://www.yhgfl.net**].

As well as providing infrastructure support to schools, RBCs offer a range of e-safety support, guidance materials, events and activities which may be of value to wider member agencies.

LSCBs may find it beneficial to make contact with their local RBC at an early stage in the development of their e-safety strategy to discuss opportunities for future working.

Further information is available on the National Education Network website [**http://www.nen.gov.uk**].

Risk assessment

A further priority action for the LSCB e-safety subgroup might be to conduct a risk assessment of the infrastructure issues across all member agencies.

In line with general health and safety practice on risk assessment, the audit should consider the infrastructure issues which could pose a risk to children – whether sufficient precautions are in place or whether more can be done to prevent the risk of harm.

Drawing on general Health and Safety Executive (HSE) guidance on risk assessment[15], we recommend the following basic five-stage process:

- Step 1: Identify the hazards
- Step 2: Decide who might be harmed and how
- Step 3: Evaluate the risks and decide on precautions
- Step 4: Record your findings and implement them
- Step 5: Review your assessment and update if necessary.

Some key questions for identifying hazards

- What technologies are used? Where? Who uses them?
- What control do member agencies have over these technologies? Do they own the technology and the connection, or are there instances where children may be communicating online using their own equipment?
- What filtering and blocking technologies are in place? How effective are these? Are they appropriate for all service users?
- Are acceptable-use policies (AUPs) in place? Do they cover all service users and all technology uses? Are they appropriate to the age of the users? Are users (or their designated parent/carer) required to sign the policy? How effective are the policies? How is the impact of the AUP monitored?

[15] See *Five steps to risk assessment* on the Health and Safety Executive website [**http://www.hse.gov.uk/pubns/indg163.pdf**].

Are processes in place for reviewing and updating the policy in line with developments in new technologies? How are breaches of the policy identified and recorded? What actions are taken when a breach occurs?

- Are technical staff aware of the issues? Are they fully aware of their proactive and reactive responsibilities for monitoring the network infrastructure in relation to e-safety?

Risk assessment of the infrastructure should be on ongoing activity for all member agencies. Although the basic e-safety risks remain the same, technologies often change, as do children's behaviours. Effective risk assessment should look towards emerging issues and technologies in an attempt to pre-empt e-safety risks before they occur.

Use of accredited services

One of the key recommendations of the LSCB e-safety subgroup might be that all member agencies use a Becta-accredited service for internet connectivity or content filtering.

The Becta Accreditation of Internet Services to Education scheme[16] 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 process makes a technical assessment of filtering services provided by ISPs 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.

Under the accreditation scheme, a product for filtering internet content must meet or exceed the following requirements.

- There must be telephone and web-based support for all aspects of the service.
- The product must block 100 per cent of illegal material identified by the Internet Watch Foundation (IWF).

[16] See Becta schools website [**http://www.becta.org.uk/ispsafety**].

- The product must be capable of blocking 90 per cent of inappropriate content in each of the following categories:
  - Pornographic, adult, tasteless or offensive material
  - Violence (including weapons and bombs)
  - Racist, extremist and hate material
  - Illegal drug taking and promotion
  - Criminal skills, proxy avoidance and software piracy.
- It must be possible to request (or make) amendments to the blocked content.

LSCBs may wish to encourage their member agencies to check the accreditation status of their ISP or filtering service and suggest investigating the possibility of accreditation if none is already in place.

Developing filtering standards

All member agencies within the remit of the LSCB should develop a local implementation plan for filtering use of the internet and communications technologies.

In terms of filtering, member agencies should use an ISP or filtering provider that subscribes to the IWF URL filtering list[17] as a minimum. URLs on that list contain potentially illegal content of child sexual abuse, but do not include potentially illegal content inciting racial hatred or any other inappropriate content. Additional filtering mechanisms must be employed to limit these risks, as appropriate to the users of the services in question.

Member agencies using an accredited service or product will already benefit from a minimum level of filtering (as outlined above) which includes the URLs on the IWF URL list. Member agencies not using an accredited service or product should seek clarification from their ISPs or filtering providers on filtering criteria and performance, and should review and monitor their effectiveness accordingly.

There are, however, issues associated with filtering, particularly for those settings offering access to technology to a wide range of users. For example, the filtering which is necessary for a child in a public setting such as a library is unlikely to be appropriate for an adult who may be engaged in legitimate research in the same setting. Equally, there is a balance to consider between the educational value of allowing access to some sites and services in certain settings (for example, social networking sites) against the potential risks. It is doubtful, therefore, that a single filtering policy could be applied to all member agencies operating under the remit of an LSCB, and the e-safety strategy should acknowledge this requirement as appropriate. Each member agency will need to tailor a filtering implementation plan to its own specific requirements.

[17] See Internet Watch Foundation website: Child Sexual Abuse Content URL List [**http://www.iwf.org.uk/public/page.148.437.htm**].

It must be stressed, however, that filtering is not a 'fit and forget' solution. No technological solution can ever be 100 per cent effective: it must be employed as just one of a range of e-safety measures within the PIES model, such as user education and robust acceptable-use policies.

Developing acceptable-use policies

In general terms, an acceptable-use policy (AUP) is a document detailing the way in which ICT facilities may (and may not) be used by service users, listing sanctions and procedures for misuse. An important educational tool, it is also useful in detailing the official position of the service provider should e-safety incidents occur (with regard to monitoring the network infrastructure, for example).

An acceptable-use policy must be wide ranging. It must consider both fixed and mobile access to the internet, technologies provided by the service itself (such as PCs, laptops, webcams and digital video equipment) and technologies owned by service users and staff but brought onto the service premises (such as mobile phones, camera phones, personal digital assistants (PDAs) and portable media players). It should be flexible enough to deal with new and emerging technologies, but should also recognise the important educational and social benefits of such tools. Further information is available on the Becta website[18].

All member agencies should develop an AUP tailored to individual users and/or stakeholder groups as appropriate.

As with filtering (see above), there should be recognition that the definition of 'acceptable use' (and, indeed, unacceptable use) may relate to the agency, context or person using the service. Member agencies may therefore wish to consider and define what constitutes acceptable or reasonable personal use within their own particular context, and document that accordingly.

In some instances it may be more appropriate to develop a number of documents as part of the acceptable-use policy – for example a management document, a document detailing acceptable staff use, and an agreement on child/parent use – possibly with differentiation within these groupings too. The most important thing is that all those governed by the policy understand the issues and their specific responsibilities as documented in the AUP, as well as the consequences and escalation path for any breaches of the policy.

There are many sample acceptable-use policies available, both online and via local authorities, which LSCBs and member agencies can use as a basis for their own policies. Remember, though, that an effective AUP needs to be tailored to the individual needs of the service and the service users, and must be thoroughly embedded in local policies and practice. It is also important to review and renew

[18] See the Becta website [**http://www.becta.org.uk**].

the AUP regularly to keep pace with both emerging technologies and emerging e-safety challenges.

Additionally, LSCBs must monitor the impact of the AUP, and support it by robust, enforceable policies and procedures. The wider work of the e-safety subgroup should help in this process.

E-safety in practice – example acceptable-use policies

South West Grid for Learning

The South West Grid for Learning (SWGfL) has produced an AUP that acts as an umbrella policy across the region. It applies to all users, children and staff, and defines what is unacceptable. Imposing this AUP at ISP level results in the deployment of a minimum standard, while still supporting schools with existing extensive policies.

For further information, see the SWGfL Safe website [**http://www.swgfl.org.uk/safety**].

Kent Council County

The Kent County Council (KCC) Children, Families and Education Directorate (CFE) has created an e-safety strategy group comprising teachers, officers, advisors, police and child protection officers. The group advises on the safe and secure use of communication technologies in schools and encourages responsible use outside school. The group has produced extensive e-safety policy guidance and linked materials including policy templates.

For further information, see the KCC ClusterWeb website [**http://www.clusterweb.org.uk?e-safety**], plus the detailed case study at **Annex A.**

London Grid for Learning

The London for Learning (LGfL) has produced a range of e-safety agreement forms for specific end-users (including primary children and adults working in schools), which could usefully be adapted for use in other settings.

For further information, see the LGfL website [**http://www.lgfl.net/lgfl/sections/safety/esafety/menu**].

Many further examples of acceptable-use policies are available online.

Although predominantly developed with an education focus, acceptable-use policies such as these can offer an excellent starting point for LSCBs and their member agencies to start considering the issues. LSCBs may wish to draw on the experiences and expertise of their educational colleagues to identify good practice approaches that might be extended to other services within the locality.

JANET

JANET is the network dedicated to the needs of education and research in the UK – the technical infrastructure that connects the UK's universities, FE colleges, research councils, specialist colleges, and adult and community learning (ACL) providers. It also provides connections between the RBCs, so forming a national schools network. The JANET network serves over 18 million end-users, so its AUP has been consistently adopted across a large user base, and effectively cascaded down to individual service locations.

For further information, see the JANET website [**http://www.ja.net/development/legal-and-regulatory/policy/index.html**].

The National Education Network (NEN)[19] is also developing a cascading AUP based on the JANET one. The intention is for this AUP to be a core set of acceptable-use statements, which individual delivery units can supplement as appropriate to their own local services, stakeholders and user groups. Further information, when available, will be published on the NEN website.

Monitoring and reporting

Member agencies must have their network infrastructure monitored regularly and consistently. There are now many software products available which can help with network monitoring, particularly tracking and identifying trends in advance of e-safety issues arising.

If e-safety incidents do occur, a robust technological infrastructure can be vitally important in providing forensic evidence and an activity trail.

Additionally, the AUP should state what monitoring and reporting of individual usage is in place. Not only can this help to encourage a culture of safe and responsible behaviour, but also transparency of approach is important to alert users to their rights to privacy (which may help to avoid complications should e-safety incidents occur).

Infrastructure staff

Staff responsible for managing the technical infrastructure in each of the member agencies will need support in their roles. They will require regular training in e-safety issues, and should be clear about the procedures they must follow if they discover, or suspect, e-safety incidents through monitoring of network activity.

[19] See National Education Network website [**http://www.nen.gov.uk**].

Infrastructure staff should understand the importance of maintaining logs, and securing and preserving the technical environment in order to be able to gather any evidence that may be required in the future. They should also know how to respond to requests for disclosure of information (see **Legislative considerations** below).

Infrastructure staff may have access to a whole range of personal, privileged or sensitive information about service users, including children, which in the wrong hands could be misused or abused. Although they may not necessarily come into direct contact with children through their work, therefore, these staff should be subject to the provisions of the *Safeguarding children and safer recruitment in education guidance*[20].

It is also worth noting that the *Safeguarding Vulnerable Groups Act 2006*[21] will introduce a new vetting and barring scheme for all those working with children and young people from 2008. In due course LSCBs and member agencies should make themselves familiar with this scheme, and revise local policies and procedures accordingly.

LSCBs and member agencies must also consider the processes to employ in a situation where infrastructure staff themselves are suspected of misusing the network and technology.

Responding to specific incidents

Technological solutions to e-safety can never be 100 per cent effective and, unfortunately, there may still be occasions when e-safety incidents do occur. There should therefore be clear lines of communication for reporting specific incidents, and this should include escalating incidents, involving other agencies and disclosure.

In developing policies and practices, the e-safety subgroup must consider various e-safety scenarios, responses and reporting mechanisms – for example:

- accidental access to inappropriate material
- deliberate access to inappropriate material
- accidental access to illegal material
- deliberate access to illegal material
- inappropriate or illegal use of email
- inappropriate or illegal use of other technologies
- deliberate misuse of the network (for example, hacking or virus propagation)
- bullying or harassment using technologies
- sexual exploitation using technologies.

[20] See *Safeguarding children and safer recruitment in education guidance* on the Every Child Matters website [**http://www.everychildmatters.gov.uk/search/IG00175**].

[21] See *Safeguarding Vulnerable Groups Act 2006* [**http://www.opsi.gov.uk/ACTS/acts2006/60047--h.htm**].

Guidance on safeguarding children and young people from sexual exploitation

The Government is developing new guidance to provide information about different forms of sexual exploitation. It is intended to help local agencies to apply the core safeguarding mechanisms in order to safeguard and promote the welfare of children and young people who may be sexually exploited.

The new guidance will supplement the statutory guidance in *Working together to safeguard children (2006)*, and replaces *Safeguarding children involved in prostitution* which was published in May 2000 as supplementary guidance to the 1999 edition of *Working together*.

This revised guidance will have a broader focus than the previous document, reflecting current understanding of the interrelated nature of different forms of sexual exploitation, including sexual exploitation in the online environment.

The guidance will be for LSCB partners, managers, practitioners and other professionals working with children. Like the earlier guidance, it will set out an inter-agency approach and should inform local policies and procedures drawn up by LSCBs, within the framework of *Working together*, to ensure that local agencies effectively address this type of abuse.

The guidance is to be published in 2008. Further details will appear on the Every Child Matters website [**http://www.everychildmatters.gov.uk**].

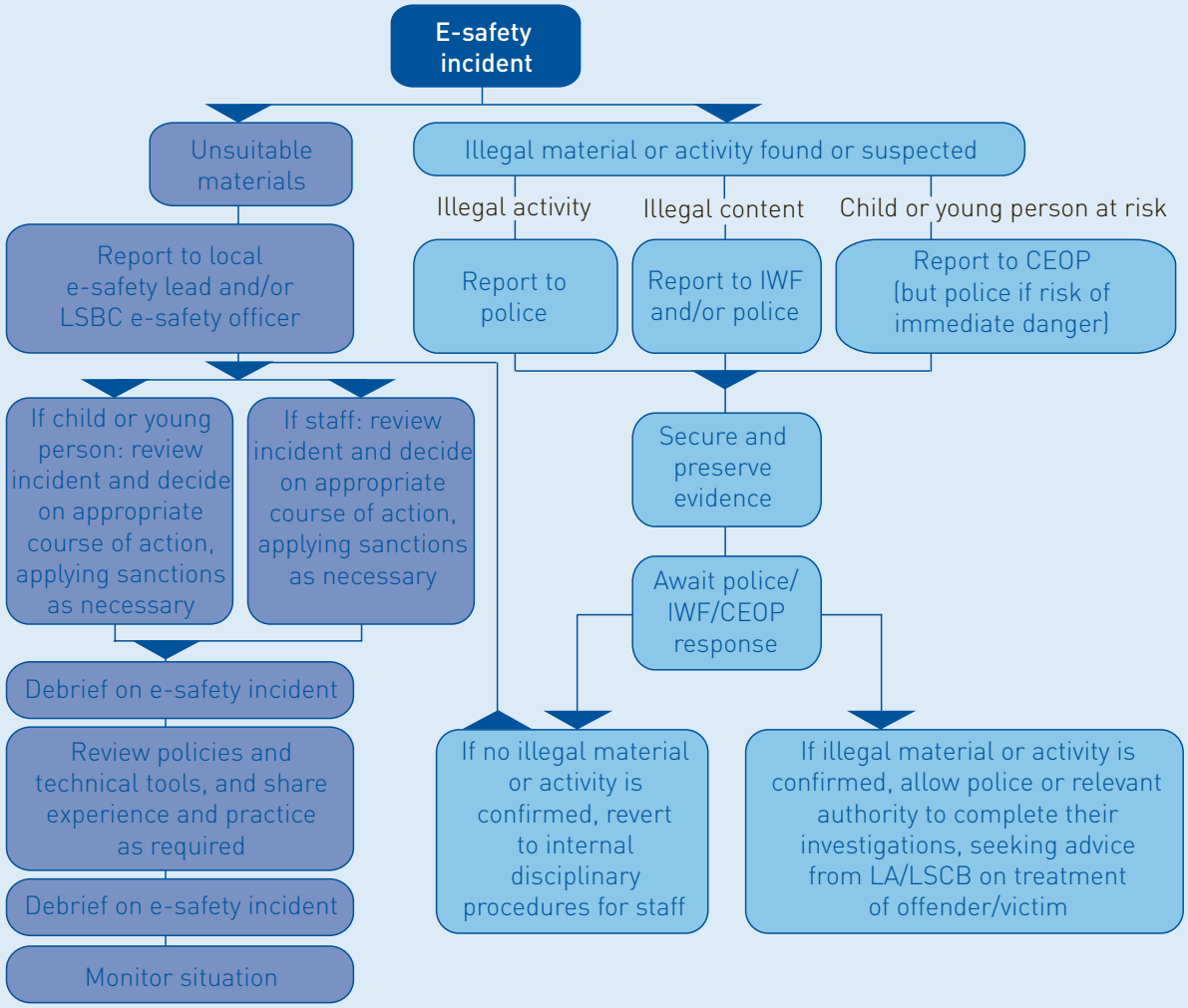
Depending on the nature of the event, different e-safety incidents will require different responses, and undoubtedly no two e-safety incidents will be exactly the same. This does not mean, however, that responses should be left to chance and circumstance: instead LSCBs and their member agencies should model general processes and procedures for responding to incidents, drawing on good practice within the wider field of child protection as appropriate. Such exercises can often be effective as both awareness raising and training tools.

Becta has developed the Framework for ICT Technical Support (FITS)[22] 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 for LSCBs and member agencies from which to develop a process 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 below:

[22] See Becta schools website [**http://www.becta.org.uk/schools/fits**].

Figure 5:
Flowchart for responding to e-safety incidents



(Reproduced from *Safeguarding children online: a guide for local authorities and local safeguarding children boards*, page 27, appendix B)

Several authorities have modelled similar flowcharts and processes for responding to incidents of concern based on their local context. You will find some examples of these at **Annex B**.

See the annexes for materials designed to help you understand e-safety infrastructure requirements and respond appropriately to specific e-safety incidents.

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 social care, the police, the Internet Watch Foundation (IWF), or the Child

Exploitation and Online Protection (CEOP) Centre) and securing and preserving evidence correctly.

In particular, member agencies must be aware of the local procedures to follow should e-safety incidents arise. This will include how and when to contact external agencies. The materials in the annexes will help LSCBs to develop their understanding in this area and also suitable local policies and practice.

Responding to allegations made online

The DCSF has recently undertaken a review of how guidance on handling allegations of abuse against those who work with children and young people is implemented. Becta responded to the review on the specific issue of online allegations.

Fundamentally, allegations made online are no different from allegations made any other way. For clarity and consistency, therefore, it is essential to investigate all allegations according to the same policies and procedures. However, for online allegations there are some specific issues, including:

- Understanding the nature of online communications, including the reach and permanency of comments made online, for offensive or misleading comments can quickly and unintentionally spread beyond control
- Ensuring appropriate focus in education and training programmes to make absolutely clear the issues of online communication, and the appropriate reporting mechanisms for allegations
- Recognising and acknowledging allegations, including what constitutes an allegation and the legal requirements for disclosure of information to support investigations of allegations
- Retention of evidence, including clarification of the legal position regarding self-publishing and information shared online while investigations are in progress
- Appropriate actions following the conclusion of an investigation, whether it is found to be false or true.

We expect the results of the consultation to be published on the DCSF e-consultation[23] website early in 2008.

Legislative considerations

There are many legislative considerations that have an impact on e-safety, particularly as these apply to the monitoring and reporting of technical infrastructure issues. Those considerations include the following.

[23] See DCSF e-consultation website [**http://www.dfes.gov.uk/consultations**].

- Data Protection Act 1998

  [**http://www.opsi.gov.uk/Acts/acts1998/19980029.htm**]

  Organisations have a right (and in the case of those providing services to children, a duty) to monitor use of their technical infrastructures to prevent them from being used inappropriately, for unlawful purposes or to distribute offensive material. However, an individual also has a right to privacy. It is the duty of any organisation that provides online access to balance these two separate rights and, in the case of children's and community services, different policies may be needed for children and adults within these settings.

  It is important to note that end-user consent is required before any monitoring or filtering of email-based content is undertaken, as covered by the provisions of the EU directive on privacy and electronic communications[24] (notwithstanding other UK legislation as detailed below). In any case, organisations should be open on the subject of monitoring the use of their technical networks, and the acceptable-use policy can be an effective way of doing this.

  Under the terms of the Data Protection Act (DPA), any data collected in the process of monitoring and reporting on the network infrastructure must adhere to the data protection principles. These state that data must be:

  - fairly and lawfully processed
  - processed for limited purposes
  - adequate, relevant and not excessive
  - accurate
  - kept no longer than necessary
  - processed in accordance with the data subject's rights
  - secure.

  Under the terms of the Act, data must not be transferred to other countries without adequate protection.

  Becta has produced a range of guidance to help institutions to comply with the requirements of the DPA in relation to the security of personal information. LSCBs and their member agencies may find it useful to review the Becta guidance.

  The *Technical specification: institutional infrastructure*[25], for example, includes detailed advice on network security, while the *Framework for ICT Technical Support (FITS)* and *FITS Operations Management (FITS OM)*[26] set out the

[24] See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [**http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_201/l_20120020731en00370047.pdf**].

[25] See Becta industry website: Technical specification: institutional infrastructure [**http://www.becta.org.uk/industry/techstandards**].

[26] See Becta schools website: Technical support [**http://www.becta.org.uk/schools/fits**].

processes schools should have in place. FITS OM includes security administration as a process in its own right.

The Information Commissioner's Office[27] is also a useful source of information.

Other legislation, as outlined below, gives further guidelines on the retention and disclosure of information.

- Regulation of Investigatory Powers Act 2000

  [**http://www.opsi.gov.uk/Acts/acts2000/20000023.htm**]

  The Regulation of Investigatory Powers Act (RIPA) sets out the legal framework for using methods of surveillance and information gathering to help the prevention of crime. It includes, among other provisions, the interception of communications, the acquisition and disclosure of data relating to communications, and access to electronic data protected by encryption or passwords. The requirement to provide access to such information is served under a RIPA notice.

  Each police force and most councils are defined as a 'public authority' to which a RIPA notice can apply. The forms of surveillance that the police and any council are entitled to authorise are covert directed surveillance and the use of covert human intelligence sources (informants). In any council, only officers of the rank of deputy chief officer and above may be designated as authorising officers under a RIPA notice. No covert directed surveillance or use of covert human intelligence sources may be undertaken without obtaining authority from such an authorising officer.

  A RIPA notice requires that third parties who are to provide information about other people subject to surveillance and investigation should be approached for that information in a highly controlled manner by means of standard forms published by the Home Office.

  It is possible that, in their role of safeguarding children, LSCBs and member agencies may be subject to the provisions of a RIPA notice. They should therefore be aware of the appropriate response if they receive such a request. It is equally important that LSCBs and member agencies do not respond to requests for communications data without a duly authorised RIPA notice: to do so, if the evidence had not been correctly requested and collected, could potentially jeopardise a case.

See **Annex C** for more guidance on responding to a RIPA notice.

- Retention of Communications Data under Part 11: Anti-Terrorism, Crime and Security Act 2001

  [**http://www.opsi.gov.uk/si/si2003/draft/5b.pdf**]

[27] See Information Commissioner's Office website [**http://www.ico.gov.uk**].

This voluntary code of practice published by the Home Office 'aims to allow for the retention of communications data to ensure that the UK security, intelligence and law enforcement agencies have sufficient information available to them to assist them in protecting the UK's national security and to investigate terrorism'. This means that ISPs in the UK retain some data under this arrangement, typically as follows:

- Subscriber information: 12 months
- Telephony data: 12 months
- SMS, EMS and MMS data: 6 months
- Email data: 6 months
- ISP data: 6 months
- Web activity logs: 4 days
- Other services: retention period relative to the service provided (for example, instant message-type services (log-on/off time) if available).

Access to any data retained under this code must be made via a RIPA notice as detailed above.

We advise LSCBs and their member agencies to seek local guidance on specific legislative issues.

Becta leading next generation learning

Developing an e-safety training strategy

Why develop an e-safety training strategy?

Key aspects of an e-safety training strategy

Establishing the existing level of e-safety awareness

Establishing the availability of e-safety training resources

Embedding e-safety in other training programmes

4

Developing an e-safety training strategy

Why develop an e-safety training strategy?

Guidance given in *Working together to safeguard children* states that, in their role of co-ordinating local work to safeguard and promote the welfare of children, LSCBs have, as one of their core objectives, to develop policies and procedures on various aspects, including training.

This is further emphasised in non-statutory practice guidance given in Chapter 11 (paragraph 11.62) as follows:

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

The development of an e-safety training strategy is therefore essential to strengthen and underpin the e-safety work of an LSCB, and should form an integral part of the wider training role of the board.

When developing your strategy, remember that, in the overall drive to safeguard children, **all** who come into contact with children in the course of their work will benefit from e-safety awareness training. This will include:

- those who listen to children (such as lunchtime supervisors and cleaners)
- those who influence children (such as teachers, parents, carers and staff in the voluntary sector)
- those who respond to incidents when children's safety has been placed at risk (such as police, social workers, child protection officers and e-safety co-ordinators).

The e-safety training strategy should address this requirement accordingly.

Key aspects of an e-safety training strategy

Key considerations in the development of an LSCB e-safety training strategy might include the following questions.

- Who needs training?
- What training should they receive? For example:
  - General e-safety and digital literacy awareness
  - Technical awareness
  - Assessing e-safety risks to/for children
  - Assessing e-safety risks posed by adults.

E-safety in practice – matrix approach to identifying training needs

Those attending the Becta e-safety working days in September 2007 felt that this matrix approach to identifying training needs might be useful:

Audience	Focus of training					
	E-safety awareness/ embedding	Technical awareness	Assessing the risks to/for children	Assessing the risks posed by adults	Other links in safeguarding children	Refresher courses/ updates
Children	✓	✓				✓
Parents	✓	✓				✓
Those who work with children	✓	✓	✓	✓	✓	✓
Those who work with adults	✓	✓	✓	✓	✓	✓
Those who work with technology	✓	✓			✓	✓
Leaders, managers and strategists	✓	✓			✓	✓

LSCBs could supplement a matrix like this with local detail as appropriate – for example, including breakdowns of specific audiences within these key groupings.

- What level should they be trained to?
- Are there any prerequisites to e-safety training? For example, child protection training?
- When should they receive the training? Considerations include induction of new staff, training of existing staff, and frequency of ongoing 'refresher' training.
- Who will deliver the training?
- How should the training be delivered?
- How will the training be validated or quality assured?
- What training resources already exist (both locally and more widely)?
- How will training be resourced?
- How will training be logged or recorded?
- How will the effectiveness of the training be monitored and reviewed?

As always, if it is to be truly effective, the strategy must be tailored to the local context. Establishing the existing level of e-safety awareness will be useful in this process, as outlined below.

Establishing the existing level of e-safety awareness

A priority action for the LSCB e-safety subgroup might be to establish the current level of e-safety awareness across member agencies and key stakeholder groups, by means of an audit or similar exercise. This may help to identify priorities for both education and training, and also to highlight other aspects of the wider e-safety strategy which need further attention.

When assessing current levels of awareness, remember that e-safety is as much about the social issues as about technical issues, covering all forms of communication devices and online interactions.

Additionally, people need to be made aware of the issues in a balanced way – alleviating fears, placing the risks within context and promoting the positive uses of technology. Equally, however, they need to recognise that the threats and dangers are very real. Addressing this balance will be a key challenge for any e-safety training strategy.

Establishing the availability of e-safety training resources

In parallel with establishing the current level of e-safety awareness within the locality, it is useful to establish the availability of e-safety training resources. Again, local educational colleagues or the RBC may be able to help here, and there will probably be local e-safety training materials in existence which LSCBs may readily draw upon.

E-safety in practice – raising e-safety awareness

Colleagues attending the Becta e-safety working days in September 2007 trialled a package of e-safety awareness-raising resources to very positive effect. Based on a series of e-safety dilemmas, the resources require users to grade e-safety scenarios in relation to the risks they present, and then to consider who may need to be involved in follow-up actions.

The resources proved excellent in promoting debate and discussion, and LSCBs may like to use them as the basis for some of their e-safety training activities. The materials include a flowchart for identifying practical actions and reflecting on practice, and a matrix for recording local contacts in the safeguarding process.

Copies of these resources are included at **Annex D**, where you will also find some notes on their use.

Several key national organisations now offer training on e-safety issues. We discuss some of these further in **Section 7**.

Embedding e-safety in other training programmes

The e-safety subgroup should also give consideration to ways of including awareness of e-safety issues in other training such as local child protection training.

Becta leading next generation learning

Monitoring and reporting on e-safety incidents

Why monitor and report on e-safety issues?

What should be monitored at member agency level?

What should be monitored at LSCB level?

The role of proactive monitoring

5

Monitoring and reporting on e-safety incidents

Why monitor and report on e-safety issues?

Monitoring and reporting on e-safety issues and incidents is important. Not only will it provide a permanent record of incidents, outcomes and actions taken, it will also provide an important tool for reflecting on and revising practice and for identifying emerging trends which can be addressed before they become problematic.

As discussed in **Section 1**, LSCBs should seek to evaluate the effectiveness of their e-safety work through a peer-review process, based on self-evaluation, performance indicators and joint audit, while individual children's services continue to be assessed through their own quality and inspection regimes. Although there is not yet any statutory requirement in this area, it is good practice to establish a monitoring and reporting framework for e-safety incidents, at both e-safety subgroup and member agency level (which ultimately feeds into the LSCB's statutory monitoring and evaluation requirements). It will also help LSCBs to meet the need to respond to specific incidents/allegations and to comply with the regulations for retaining communication data (see **Section 3** above).

Reports of e-safety activity can also prove invaluable in establishing the longer-term effectiveness of the LSCB e-safety strategy. We discuss this further in **Section 6**.

What should be monitored at member agency level?

The e-safety subgroup may wish to suggest a minimum e-safety dataset which should be maintained at member agency level.

As an absolute minimum, member agencies should establish an e-safety incident log. This should record factors such as the following:

- A description of the e-safety incident
- Who was involved?
- How was the incident identified?
- What actions were taken, and by whom?
- Conclusions to the incident.

The use of model incident flowcharts (see figure 5 on page 11 of **Section 3** above) will help in this process and, most importantly, will help member agencies to recognise when they have reached the limit of their responsibilities – the point at which they must escalate an e-safety incident to another appropriate agency.

Member agencies should review their incident logs regularly to identify where revisions to policy and practice are necessary to minimise the risk of recurrence of similar incidents.

It may also be beneficial for member agencies to include e-safety as a standing agenda item at team meetings. This will help to make certain that they review

issues, policies and processes regularly, and that they maintain the profile of e-safety across all agency work.

What should be monitored at LSCB level?

Although LSCBs will not need to receive all monitoring reports from member agencies, some key reports – such as the type and number of e-safety incidents occurring across all member agencies – may be collated at LSCB level. This will help to give an overview of the local e-safety landscape, and may help to identify future priorities for policy and practice. When establishing their strategy, e-safety subgroups should consider setting up a monitoring and reporting framework, and communicate this to their member agencies.

Most e-safety incidents will probably be reasonably low level and can readily be resolved at member agency level, but the potential occurrence of serious e-safety incidents is nevertheless a very real prospect. Because of this, the e-safety subgroup may wish to establish a mechanism for reporting and reviewing all serious e-safety incidents, and it may be appropriate to make it a standing agenda item for e-safety subgroup meetings.

When reviewing serious e-safety incidents, the e-safety subgroup should consider:

- Why did the incident happen?
- Are there any measures which could have prevented the incident?
- What was the response? Was the response effective? Could/should anything else have been done?
- What lessons have we learned from the incident? How should we disseminate those lessons to inform future practice, both locally and nationally? How should local policies and practice be adapted as a result?

The role of proactive monitoring

The sections above outline the importance of reactive monitoring, but proactive monitoring can be just as important to a successful e-safety strategy.

Proactive monitoring of the digital landscape within a given area (for example, by determining the percentage of young people having internet access at home or the percentage with social networking profiles) can help to establish how young people in the locality view and use digital technologies, what their concerns are, and any emerging issues.

Not only will such proactive monitoring help to keep e-safety at the forefront of local thinking, but it can also produce key performance indicators with which to review and revise the e-safety strategy in the future.

Becta leading next generation learning

Monitoring the impact of the e-safety strategy

Why monitor the impact of the e-safety strategy?

What are the measures of success?

Reflecting on practice

6

Monitoring the impact of the e-safety strategy

Why monitor the impact of the e-safety strategy?

Working together to safeguard children states that one of the core LSCB objectives in ensuring the effectiveness of their co-ordination of local work to safeguard and promote the welfare of children is to monitor the effectiveness of what is being done (chapter 3, page 75, figure 1: LSCB objectives and functions).

More recently, the DCSF priority review of LSCB progress[28] recognised that LSCBs need a better understanding of how well they are doing. Paragraphs 10.10 and 10.11 in the document state:

> 'The Government is seeking to address this by looking at the scope for national and local measures of safeguarding... Over time we hope to see a move towards more outcome-focused measures of safeguarding, rather than processes or inputs.
>
> In the shorter term the Government plans to make sure LSCBs have access to a benchmarking toolkit which helps them to think through their own effectiveness. This will help LSCBs to understand and to think through "what good looks like" and to measure themselves against statements of practice which complies with guidance and which helps them towards effective delivery of their functions and achievement of the safeguarding outcomes.'

As this area of evaluation matures, we hope that models for evaluating e-safety effectiveness will also emerge. Becta will continue to support both the DCSF and the LSCBs in this process.

In the meantime, LSCBs should develop their own local processes for monitoring the impact of their e-safety strategy.

What are the measures of success?

In order to monitor effectiveness, LSCBs must first establish some baseline data on which to measure their progress. The various auditing exercises discussed in the earlier sections of this document may help in this process (see **Section 2** page 4–5 and **Section 3** page 1–2).

The e-safety subgroup must then establish its own criteria for evaluating the impact of the strategy (including frequency of review), strongly linked to its aims and objectives. Factors to consider might include the following:

- The number of member agencies with an acceptable-use policy in place
- The number of member agencies with an identified e-safety lead
- The number of member agencies using an accredited internet service provider
- The number of member agencies with a filtering and monitoring plan in place

[28] See *Local safeguarding children boards: A review of progress*, available on the Every Child Matters website [http://www.everychildmatters.gov.uk/lscb].

- The number of member agencies with a local e-safety awareness and training plan in place.

Judgements of effectiveness against other factors, such as the number and nature of reported e-safety incidents, may be more difficult to make – particularly in the short term. For example, an increase in the number of e-safety incidents reported locally may be an indicator that the e-safety strategy is having a positive impact rather than the reverse. This is because an effective e-safety strategy will increase awareness of issues, children will feel more comfortable discussing their concerns with adults, adults will become more skilled at identifying potential situations giving cause for concern, and member agencies will become more adept at monitoring and responding to infrastructure incidents, both proactively and reactively. In order to understand fully the significance of indicators such as these, LSCBs will need to take a longer-term view of effectiveness.

Reflecting on practice

It is vitally important that the e-safety subgroup and its member agencies regularly reflect on their practice in order to revise strategies and policies as appropriate. This will enable the LSCB to respond more effectively to the frequently changing e-safety and safeguarding landscape.

Becta leading next generation learning

Sources of external e-safety support

Child Exploitation and Online Protection Centre

Insafe

Internet Watch Foundation

Kidscape

Know IT All

NSPCC and related services

Stop it Now!

University Certificate in Child Safety on the Internet

Virtual Global Taskforce

Sources of external e-safety support

In addition to the local support network that LSCBs and member agencies can draw upon for their e-safety work, there are some external agencies that can help. Their support may take the form of providing training on e-safety issues, responding to specific e-safety incidents or supporting the key stakeholders in a child life. Some of these we describe briefly below.

LSCBs that want to develop their own extended lists of both internal and external support services will find useful resources in **Annexes B, C, D** and **E.**

- ## Child Exploitation and Online Protection Centre

  [**http://www.ceop.gov.uk**]

  The Child Exploitation and Online Protection (CEOP) Centre is a law enforcement agency that aims to tackle child sex abuse wherever and whenever it happens. Part of its strategy for achieving this is to give internet safety advice for parents and carers, training for educators and child protection professionals, and a 'report abuse' button for reporting abuse on the internet.

  We give below brief details of some of these services.

Thinkuknow – online safety for young people and their parents

[**http://www.thinkuknow.co.uk**]

The CEOP Thinkuknow website has a range of information on online safety for young people, with key topics including mobiles, gaming, social networking, chatting, podcasts, blogs, and peer-to-peer technologies.

The content of the site is based on three key messages:

- How to have fun online
- How to stay in control online
- How to report a problem online.

A section of the website specifically for parents and carers aims to help them understand more about what their child may be doing online.

In addition to being a good general resource on current e-safety issues, this site is one that LSCBs, as part of their awareness-raising work, may like to promote to children, parents and carers.

The site also has a prominent link to the CEOP service for reporting suspicious behaviour online with or towards a child (see **Reporting abuse** below).

Training for educators

[**http://www.thinkuknow.co.uk/teachers**]

Through the Thinkuknow education programme, CEOP offers training for those working with children aged between 11 and 16. The training is available to anyone who has a professional role in child protection, education or law enforcement – which can include police officers, teachers, social workers, child protection specialists and people from children's charities and voluntary organisations.

Once trained, educators are able to deliver the Thinkuknow programme directly to children. Completion of the CEOP Ambassador Training scheme will allow educators to cascade the training to colleagues.

Training for child protection professionals

[**http://www.ceop.gov.uk/training/courses.html**]

CEOP works alongside colleagues in the criminal justice and child protection agencies in the UK and abroad to add value to existing services and support the professionals working in this area.

The centre offers a series of specialist training courses aimed at professionals who:

- conduct criminal investigations where the sexual abuse of children is a factor
- manage offenders in the community or within the justice system
- take responsibility for safeguarding children from sexual predators.

The training courses are designed to help delegates to understand clearly the nature of sexual offending and to develop the skills and knowledge that can better equip professionals to deal with the difficult and distressing nature of such crimes. One of the courses deals specifically with internet sex offenders.

Reporting abuse

CEOP provides a facility, in association with the Virtual Global Taskforce, for reporting any inappropriate or potentially illegal online activity towards a child. This might be an online conversation with someone who a child thinks may be an adult, who is treating a child in a way which makes them feel uncomfortable, or who is trying to meet a child for sex.

If a child is in immediate danger, dial 999 for police assistance.

There are prominent reporting links from the CEOP website, the Virtual Global Taskforce website and the Thinkuknow website. A reporting link is also available as a tab option in MSN Messenger.

- ### Insafe

[**http://www.saferinternet.org**]

E-safety is a concern in every country in the world, and, although national priorities and responses vary, there are common concerns relating to content, communication, contact and commerce.

Insafe brings together expertise and best practice from national nodes (CEOP in the UK) that co-ordinate internet safety awareness in Europe. The network is set up and co-funded within the framework of the European Commission's Safer Internet plus Programme and co-ordinated by European Schoolnet [**http://www.eun.org**].

The Insafe portal has resources, newsletters, guidance, information and activities for children, teachers and carers as well as free posters and awareness materials in a range of languages.

The annual Safer Internet Day takes place in February and brings together awareness activities, campaigns and competitions throughout Europe.

- ## Internet Watch Foundation

[**http://www.iwf.org.uk**]

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

The IWF website gives an overview of the IWF URL list of online child sexual abuse content, which should be included as an absolute minimum in internet filtering services (see **Section 3** above). You can find details on the IWF website [**http://www.iwf.org.uk/public/page.148.htm**].

The IWF also gives guidance for IT and HR professionals on how to deal with any images of child sexual abuse found on an organisation's servers, with specific reference to the Sexual Offences Act 2003. An online guide to best practice [**http://www.iwf.org.uk/public/page.137.htm**] contains a handy checklist which LSCBs may usefully incorporate in staff acceptable-use policies.

- ## Kidscape

[**http://www.kidscape.org.uk**]

Kidscape is a UK charity committed to keeping children safe, established specifically to prevent bullying and child sexual abuse. The charity works with children and young people under the age of 16, their parents and carers, and those who work with them. Its aim is to help equip vulnerable children with practical non-threatening knowledge and skills in how to keep themselves safe and reduce the likelihood of future harm.

Kidscape also offers a range of training programmes both for children and for those who work with them, covering areas such as the following:

- Child protection
- Anti bullying
- Personal development
- Promoting positive behaviour
- Staff development.

Kidscape trainers work extensively with a range of organisations including schools, local authorities and related groups such as parent-teacher associations (PTAs), governors, midday supervisors, nursery nurses and initial teacher trainers, and also with service groups such as police, youth workers, social workers, children's homes, leisure centre staff and foster carers.

- ## Know IT All

[**www.childnet.com/kia**]

Know IT All is a set of interactive resources developed by children's charity Childnet International to educate young people, parents and teachers about safe and positive use of the internet.

- ## NSPCC and related services

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

NSPCC registered charity numbers 216401 and SC037717

The NSPCC's purpose is to end cruelty to children. Its vision is of a society where all children are loved, valued and able to fulfil their potential. It is the only UK charity with statutory powers to protect children at risk, authorised under the Children Act 1989 to apply for care and supervision orders in its own right.

The NSPCC offers a range of advice and support services for children, parents, carers and professionals. We give below a brief outline of some of those services.

Children and the net

Children and the net is a basic awareness CD/DVD training programme on the safeguarding implications of ICT for practitioners working with children or adult offenders. Commissioned by the Home Office and produced by the NSPCC in partnership with NCH, this training programme is for all staff in agencies working with children and young people. The resource is part of a wider offering of child protection and safeguarding training materials developed by the NSPCC.

[**http://www.nspcc.org.uk/Inform/trainingandconsultancy/learningresources/learningresources_wda47881.html**]

ChildLine

[**http://www.childline.org.uk**]

NSPCC services include ChildLine, 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.

There4me.com

[**http://www.there4me.com**]

There4me.com is an online advice and information service specifically aimed at children aged 12 to 16. It covers topics such as internet safety, abuse and bullying. Services include message boards, a private online inbox, and 'real time' one-to-one counselling with NSPCC advisors.

Child Protection Helpline

The NSPCC Child Protection Helpline offers advice and support to any adults concerned about the welfare of a child. The helpline is a free, confidential service open 24 hours a day, seven days a week on **0808 800 5000**.

- ### Stop it Now!

[**http://www.stopitnow.org.uk**]

Stop it Now UK & Ireland is a campaign, managed by the Lucy Faithfull Foundation, which aims to prevent child sexual abuse by raising awareness and encouraging early recognition and responses to the problem by abusers themselves and those close to them. It does this by establishing regional and local projects, disseminating information and providing a helpline.

The Stop it Now! freephone helpline on **0808 1000 900** offers confidential advice and support to adults who may be unsure or worried about their own thoughts or behaviour towards children, or the behaviour of someone they know, whether that person is an adult or a child.

Experienced advisors are available to discuss concerns and can offer confidential advice and guidance on an appropriate course of action.

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

[**http://www.uclan.ac.uk/host/cru**]

This distance-learning training course for teachers, education and child services professionals aims to enable them to promote safe and responsible use of internet and mobile technologies and services. The Cyberspace Research Unit (CRU) validates the course in partnership with the University of Central Lancashire (UCLAN).

- ### Virtual Global Taskforce

[**http://www.virtualglobaltaskforce.com**]

The Virtual Global Taskforce (VGT) is made up of world-wide law enforcement agencies working together to fight child abuse online. The aim of the VGT is to build an effective, international partnership of law enforcement agencies that helps to protect children from online child abuse.

A section for young people has links to a range of useful resources, and the site also features a direct link for reporting abuse.

Becta leading next generation learning

Other sources of support

Cross-LSCB working

Becta Safetynet mailing list

Becta e-safety resources online

Becta e-safety publications

Other sources of support

E-safety is not something that LSCBs, or indeed their member agencies, need 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.

Cross-LSCB working

Where possible, opportunities for cross-LSCB working should be investigated to develop effective strategy and practice, and to support the involvement of member agencies that may be operating across a wider area. As stated in *Working together to safeguard children* (paragraph 3.72):

> 'Where boundaries between LSCBs and their partner organisations – such as the health service and the police – are not co-terminous, there can be problems for some member organisations in having to work to different procedures and protocols according to the area involved, or having to participate in several LSCBs. It may be helpful, in these circumstances, for adjoining LSCBs to collaborate, as far as possible, in establishing common policies and procedures, and joint ways of working, under the function of "Co-operation with neighbouring children's services authorities and their Board partners".'

In the field of e-safety, which by its very nature has no geographic boundaries, this may in fact be essential.

It may also be useful for LSCBs to foster relationships with neighbouring authorities in the development of training materials and self-evaluation tools, in order to benefit from pooling resources and establishing a framework for benchmarking and peer review.

Becta Safetynet mailing list

[**http://lists.becta.org.uk/mailman/listinfo/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.

We plan to post via the Safetynet mailing list any updates or additions to information in this document, or additional opportunities arising from this strand of work.

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 acceptable-use policy.

Becta e-safety resources online

[**http://www.becta.org.uk/localauthorities/safety**]

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

We update the site regularly with information on emerging technologies and issues, and there are a number of examples of good practice in areas such as email, chat rooms and acceptable-use policies. We shall also post any updates or additions to information in this document online.

Becta e-safety publications

[**http://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 specifically for local authorities and LSCBs are:

Safeguarding children online: a guide for local authorities and local safeguarding children boards

This contains a series of practical checklists for local authorities and, more specifically, for local safeguarding children boards on developing a co-ordinated approach to e-safety across all services within their remit.

A summary version is also available.

The following titles have more of an educational focus, but nevertheless contain some useful background information and resources which LSCBs could adapt for their own use:

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 publication 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.

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

This publication gives 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. It outlines the risks, suggests a policy framework for schools and gives an overview of the internet safety responsibilities of all the key stakeholders in a child's education. It also includes practical strategies to follow should schools encounter problems.

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.

Becta leading next generation learning

Contents

Annexes

Guidance on using the annex materials

In the annexes you will find a range of resources and materials to help LSCBs to clarify their thinking on e-safety issues.

Some materials are for use as training resources. Others are outline operational documents which LSCBs may adapt and complete with content and contacts as appropriate to their services. We have also included some case-study materials to illustrate how different authorities have approached e-safety issues, and to illustrate specific safeguarding scenarios that have an e-safety aspect.

Where appropriate, each annex gives instructions on using the resources it contains.

Becta leading next generation learning

A

Local authority case studies

Local authority case study 1
Brent – an e-safety roadmap

Local authority case study 2
London Borough of Havering

Local authority case study 3
E-safety in Kent

Thanks to colleagues in these authorities for sharing this material.

Local authority case study 1

Brent – an e-safety roadmap

Anna Janes, Head of Systems and Performance Management and LSCB lead for e-safety, and Jonathan Baggaley, Principal Information Officer, outline the London Borough of Brent's strategic approach to e-safety.

Introduction

Since April 2006, through our Local Safeguarding Children Board (LSCB) and alongside our partners, we in the London Borough of Brent have been navigating our way through the landscape of e-safety.

Working together 2006 placed a clear responsibility on LSCBs to play a key role in addressing e-safety. As a result, we have approached the issue from this multi-agency perspective by creating a formal sub-committee of the LSCB to consider how we can safeguard children in a digital world. Such a multi-agency approach has been essential, for this is a vast and fast-shifting area with implications for many areas of children's lives and professionals' practice.

In considering e-safety, it quickly becomes apparent that the issues raised are not restricted to questions of appropriate use of technology in classrooms or at home. Rather, the increased use of ICT by children, young people and society as a whole is affecting the very way in which people communicate and the nature of communication itself. It is a defining feature of modern life. Children's and young people's understanding of personal relationships, identity and appropriate behaviour are all potentially affected and we must be alive to the risks that this entails. Any e-safety strategy cannot therefore simply look at the technology and propose technological solutions. The scope of 'e-safety' as a 'domain' of safeguarding has surprised many of us, as we realise that the boundaries between e-safety and other areas of safeguarding are not necessarily fixed.

For many professionals the question of e-safety can therefore feel like frightening and unexplored territory, particularly as the media profile of risks such as grooming and cyber-bullying increases. While this is an understandable response, one should be clear that an understanding of safeguarding is all that is required to understand e-safety. While it is a challenge for all of us working in child-focused services, we have found that it is not one to be shirked. This report is an attempt to explain how we have begun to put this into practice in Brent.

The Brent context

The London Borough of Brent is a complex mix of cultural diversity, sharp socio-economic divides and a vast and growing young population. The population is estimated to be around 276,000 and growing, with nearly 25 per cent under nineteen years of age. This proportion is set to increase over the next ten years.

As in any local authority, our strategies must take into account our particular demographic profile and we must be alert to any specific issues that may arise out of it. An example of this in the case of e-safety is the imperative placed upon us by our cultural diversity to find out how different groups are engaging with ICT and what implications this might have for safeguarding. As one of the most culturally diverse areas in the country, Brent is one of only two boroughs where black and minority ethnic groups are in the majority.

Children and young people in Brent

Brent has sharp socio-economic divides, with some acute concentrations of deprivation. Nearly 15 per cent of our population lives in some of the most deprived wards in the country. Nearly a quarter of Brent's households are classified as overcrowded. Over a third of Brent's children live in low-income households in receipt of council tax benefit. Nearly a third are entitled to free school meals, and the proportion is rising. Nearly a quarter live in social housing. Over a fifth are in single-adult households.

Three quarters of Brent's school children are of black or minority ethnic heritage, and our children speak over 130 languages. The profile of Brent's young population continues to change. There has been a slight decline in the numbers of children of Indian heritage and an increase in children of mixed heritages. The largest single group in our primary schools is now Black African, with nearly half of these children being Somali.

Most of our children live in settled, moderately prosperous circumstances, often in extended families. These families are often part of close-knit communities which give children a sense of belonging and cultural identity. Many children and young people attend supplementary schools, Sunday schools or other religious and cultural groups outside their formal schooling. A significant proportion of children come from families on the move: four in ten children in Year 6 were not in their current school or not in this country in Year 1.

There are 56 primary schools in Brent – 33 community primary schools, 20 voluntary aided (VA) schools and three foundation primary schools. Brent also has four nursery schools and five special schools. Our 14 secondary schools consist of nine foundation schools, four voluntary aided (VA) schools, and one city academy.

Brent Children and Families department

As in many local authorities in England, the Children Act 2004 was followed in Brent by a period of restructuring. Out of this, in July 2005, came the Brent Children and Families department. It was the result of the merger of children's social services and the children's services divisions of Education, Arts and Libraries. Under the Director of Children's Services, this newly formed department has four divisions:

- Children's social care
- Achievement and inclusion
- Strategy and partnerships
- Finance and performance.

The thinking behind such a change was to combine all child-focused services under a single umbrella to enable a holistic approach to supporting children, young people and their families in Brent.

Following the creation of the new department, a post of Head of Systems and Performance Management was created, responsible for monitoring and evaluating the performance of the entire Children and Families department. This role was uniquely placed to provide an overview of the performance of the whole service.

Also in accordance with the Children Act 2004, Brent created its Local Safeguarding Children Board (LSCB) from what had previously been its local Area Child Protection Committee. There is a statutory requirement for an LSCB to have several attendant sub-committees, one of which is the Monitoring and Evaluation sub-committee which has responsibility for ensuring that all agencies in the borough work in co-operation to safeguard children. The Head of Systems and Performance Management was assigned deputy chair of this sub-committee, so extending their remit to monitoring not only performance within the Children and Families department, but also that of partner agencies in Brent.

E-safety in Brent – how did it start?

The creation of the new Children and Families department brought genuine changes to our working practices, bringing colleagues from social care and education together in unprecedented ways. Of course, this was not without difficulty, as people from each sector had to grapple with the different imperatives governing each other's services. Gradually, however, people began to understand and appreciate each other's roles and closer working allowed the sorts of 'chance' meetings and sharing of ideas that eventually enabled e-safety to take its rightful place on Brent's agenda.

One of the groups to emerge in this new era of partnership working was the Children and Families ICT Strategy group. This group is responsible for developing a departmental strategy which sets out how we plan to use ICT to support our identified priorities. The Head of Systems and Performance Management was the designated social care representative.

With hindsight and the benefit of a year thinking about e-safety, it could seem inevitable that the question of e-safety would arise out of a group concerned with positive promotion of ICT, as the two are inextricably linked (although this does not necessarily happen naturally). At that time, the end of 2005, e-safety did not have the high profile it does now and even the 'techies' in the group would be the first to admit that they had not considered the wider implications of children's increased use of ICT and our promotion of it.

In the end it was a minor point of information under 'any other business' on the agenda which brought e-safety to the attention of the group. A colleague had attended a Becta conference in November 2005. He mentioned that there had been an interesting presentation about e-safety, and passed on a copy of Becta's *Safeguarding children in a digital world*, which he had picked up at the conference. We decided to examine the issue further.

Thanks to the work of Becta, and the clear responsibility felt by schools, the e-safety agenda has often been driven by agencies involved in education. Reading *Safeguarding children in a digital world*, however, revealed that there were considerable issues pertaining to social care and other agencies that the LSCB was involved with, and that these needed to be addressed at a wider and higher level. The new *Working together*, which places a clear responsibility on LSCBs to take this forward, had not at this stage been published, but the LSCB seemed like the ideal forum for this. E-safety was therefore included on the agenda for the first LSCB meeting of 2006.

Recommendation: If you are a member of the LSCB then you can take e-safety to the board directly. If not, then we strongly suggest you persuade a member of the board or a member of one of the sub-committees to take it up and get it on the agenda. If necessary you could go and present to the members, setting out the risks, the possible safeguards and how the LSCB could take a lead role in planning strategy for the local area. Don't forget that *Working together* clearly states that LSCBs have responsibilities in this area.

Putting e-safety on the agenda

Anybody starting to consider e-safety can quickly become overwhelmed by the apparent enormity of the task. Before even considering any practical actions to take, one can be baffled by the many new online practices which children and young people are making their own. Be it instant messaging or social networking, blogs or podcasts, there can appear to be a whole new vocabulary to learn before one even considers what risks these new practices may pose to children and young people.

It is of course of the utmost importance that anyone considering taking on e-safety for a local authority has a solid understanding of the fast-moving world of the web, but this doesn't mean that e-safety is an area for ICT professionals only. Far from it, for the experience of practitioners from social care, education, the police, health services and the voluntary sector in safeguarding children will be far more important to an e-safety strategy than the knowledge of how TCP/IP works. First, however, professionals must be convinced of the importance of the area.

In order to get e-safety on the agenda of the Brent LSCB, and to make professionals aware of the importance of this area, it was necessary for us first to do our research. Without knowing what the risks were, and what we might be able to do to safeguard against them, we would never be able to convince other professionals of the importance of taking some action on the issue.

At this point our knowledge of the issues behind e-safety and its scope was miniscule. All we really knew was that it was a growing area that was posing a risk to children and as such we had to consider it within the wider context of safeguarding.

The Principal Information Officer of Children's Social Care conducted some background research to help us get to grips with what was clearly a huge and complex area, to produce a paper which could be presented to the board members.

Recommendation: Do your research but don't be put off by the technology. If you understand safeguarding, then you understand e-safety.

Research

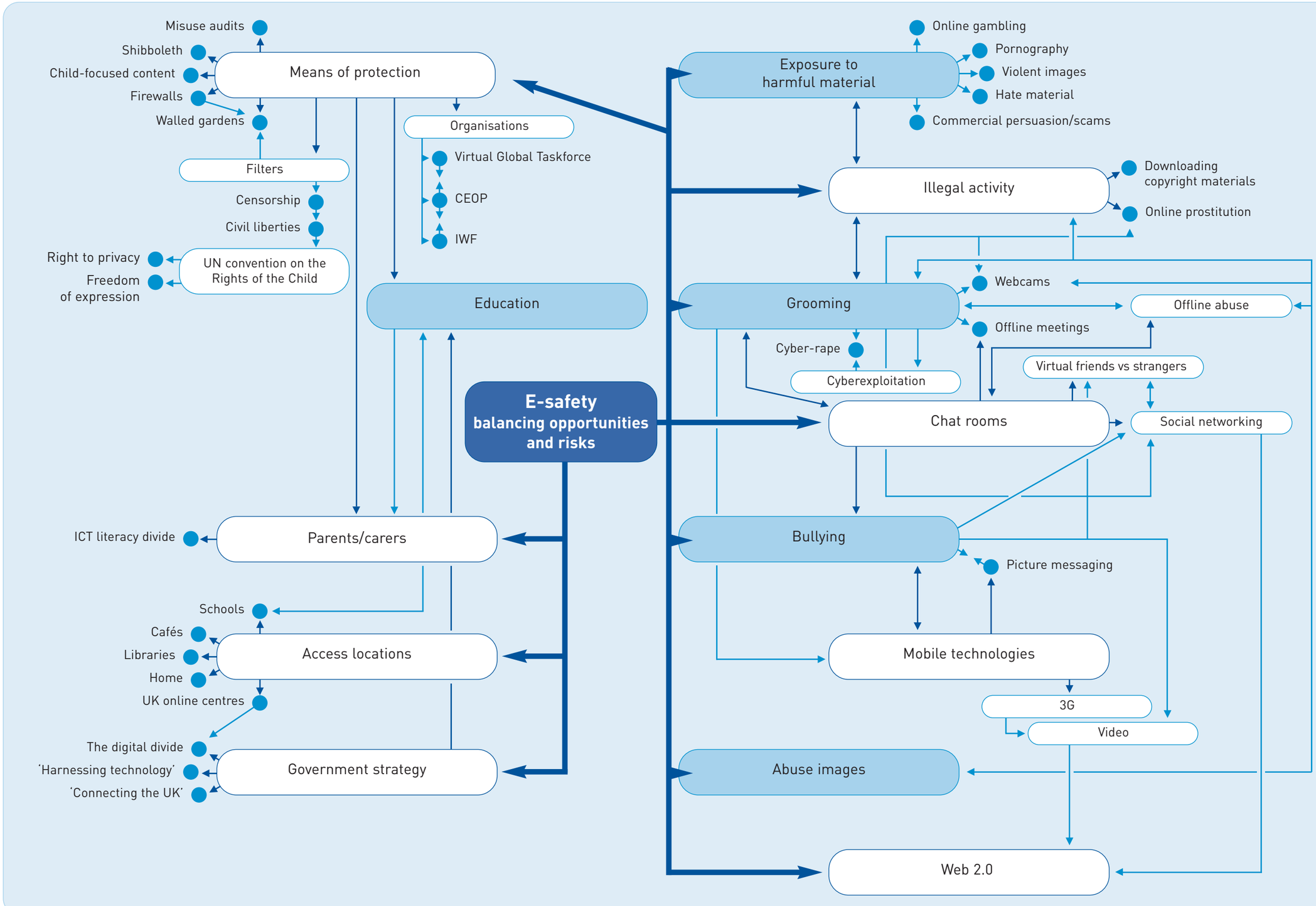
Prior to the launch of CEOP in April 2006 and the publication of *Working together* in the same month, there was very little guidance aimed at local authorities looking to tackle e-safety issues from a multi-agency perspective. Indeed, it appeared that co-ordinated approaches to the subject were very much in their infancy.

Despite the excellent work of Becta, and in particular its paper *Safeguarding children in a digital world*, it was difficult to find examples to follow of local authorities taking a lead in e-safety. Much of the advice and guidance available was largely aimed at educationalists and was therefore not broad enough. Further, there appeared to be no single authoritative body from which to take advice and guidance. As a result not only did our research have to identify the risks posed to children by increased use of ICT but also to identify the key players in the field, how they related to one another and how our strategies might interact with them.

Having considered a wide range of sources from government strategy like *Harnessing technology* to academic research like *UK children go online*, the Principal Information Officer constructed a mind map (see overleaf). The aim of this was to give a broad overview of e-safety, the risks, possible solutions and any issues which might affect one's approach to it like 'children's right to privacy' or the 'digital divide'. As a visual aid for demonstrating the scope and importance of e-safety, it was invaluable.

It was armed with this map and a short paper setting out the key issues in layman's terms that we approached the LSCB, ready to get e-safety onto Brent's agenda.

Recommendation: When getting colleagues engaged with e-safety try using simple graphics to illustrate the breadth and depth of this area without baffling them with its complexity. Try using some key headlines and perhaps a few terms they may be unfamiliar with which will make them sit up and take notice – for example *cybersexploitation*.


E-safety
balancing opportunities
and risks
Means of protection
Misuse audits
Shibboleth
Child-focused content
Firewalls
Walled gardens
Filters
Censorship
Civil liberties
Right to privacy
Freedom
of expression
UN convention on the
Rights of the Child
Organisations
Virtual Global Taskforce
CEOP
IWF
Education
Parents/carers
ICT literacy divide
Access locations
Schools
Cafés
Libraries
Home
UK online centres
Government strategy
The digital divide
'Harnessing technology'
'Connecting the UK'
Exposure to
harmful material
Online gambling
Pornography
Violent images
Hate material
Commercial persuasion/scams
Illegal activity
Downloading
copyright materials
Online prostitution
Grooming
Webcams
Offline abuse
Offline meetings
Cyber-rape
Cyberexploitation
Virtual friends vs strangers
Chat rooms
Social networking
Bullying
Picture messaging
Mobile technologies
3G
Video
Abuse images
Web 2.0

Group membership

Writing an e-safety strategy will require skills and experience from many fields including child protection, education, IT security, policing and communications. In order to construct and implement an e-safety strategy, group members must have knowledge of the structures of educational settings in a local authority and other services being provided to children and young people in both statutory and voluntary areas. As a result, any e-safety group must comprise the right people and who the 'right' people are may not be immediately obvious. They might not be the 'usual suspects'.

When working out whom to invite to join the group we started by considering access points: access points to the internet and access points to children and young people. Which agencies were providing internet access to children and young people? Which agencies would give us access to children and young people for education campaigns or research?

Our initial membership therefore was:

- Head of Systems and Performance Management (Children and Families Department)
- Principal Information Officer (Social Care)
- London Grid for Learning
- Education Child Protection Advisor (Children and Families Department)
- IT Security Manager (LA Corporate IT)
- Detective Inspector, Child Abuse Investigation Command (Metropolitan Police).

The group has since expanded to include representation from City Learning Centres, the Primary Care Trust, the School Improvement Service, the Extended Schools Programme and Arts and Libraries.

Recommendation: Get your group membership right and think laterally about whom it should include. Expect and accept that by necessity the membership could change.

The remit of the group

At its first meeting, the LSCB e-safety sub-committee agreed its terms of reference as follows:

- To build on the work of Becta, the Home Office and CEOP in raising awareness about the safe use of information communication technologies by children
- To take a lead role in the development and delivery of training and education programmes (including linking with CEOP)
- To devise an overarching e-safety strategy which forms the basis for other agency strategies

- To support all agencies involved in the safeguarding of children in developing policies, procedures and strategies related to e-safety
- To ensure that the LSCB monitors that individual strategies are in place by means of the Monitoring and Evaluation sub-committee.

Engaging local stakeholders

It quickly became evident that if we were to meet these stated aims effectively then we would need to engage other local stakeholders, make them aware of the issues and get their support in tackling them.

We broadly categorised these stakeholders into five groups:

- Education
- Health
- The third sector
- Youth
- Crime and justice.

Education

As is well known, schools have an absolutely vital role to play. They have a clear responsibility not simply to ensure that the ICT systems used within their boundaries are secure and used appropriately, but also to educate children about the risks they may face online. Schools also provide direct access to parents, a crucial factor in getting e-safety messages into the home.

When we first formed our group we really had no idea to what extent schools in our area were tackling the issue of e-safety, if at all. We therefore arranged visits to a couple of local schools to talk informally with teachers. Inevitably the first teachers we arranged meetings with were ICT subject leaders, despite our awareness that e-safety should be a whole-school issue. Our initial meetings bore out our suspicions that at that time e-safety would be considered the preserve of the ICT department.

Even within ICT departments, though there was an awareness of some of the risks, there was very little being done to educate children about them. The primary focus was on acceptable-use policies and filtering of school networks. Where there had been lessons on internet safety, this had been due to individual teachers taking the initiative. This was perhaps understandable as, although there were available materials for planning lessons, little had been done in our area to make teachers aware of them and their importance.

In July 2006 all members of our group attended training in CEOP's Thinkuknow education campaign. Not only was this an excellent resource, but also it provided us with something to present to schools to engage them in the issue as a whole. We clearly needed support in this at a strategic level and our opportunity to gain this came with the Brent Headteachers' ICT Conference.

This conference was organised by a member of our group in his role as Brent ICT advisor to education. As a result he was able to make its primary focus e-safety and locate it at CEOP, who allowed us to use their training room as a venue. This was a key milestone in engaging the schools, as 60 headteachers came to the national centre for safeguarding children online and saw presentations from CEOP and ourselves. Overwhelmingly headteachers voiced a desire for action and for support in tackling e-safety issues.

The interest from headteachers led to many direct links with schools in the borough. We were invited to attend a number of parents' evenings, to give talks to teachers and in one school to pilot Thinkuknow with a group of Year 7 students.

Health

The role that health services have to play in e-safety is less obvious than that of education. Indeed, as we initially focused on education, for some time we had no representation from health on our sub-committee. Having invited one of our child protection nurse advisors to join the group, however, we soon found that here was another area with huge potential for bolstering our e-safety strategy.

Our first action has been to attempt to engage health visitors in the issues. Following the birth of every child, the family is assigned a health visitor, making them a perfect channel for getting information to parents at the earliest possible opportunity. As a result we have attended the Health Visitors' Forum to begin the process of putting e-safety on their agenda. We are also looking at incorporating e-safety into health visitors' child protection training and providing e-safety information in the guidance given by health visitors to new parents. This guidance covers a wide range of issues, including safety in the home, and e-safety sits naturally alongside this. Though this may seem premature, new parents are given guidance covering all stages of a child's development and we feel that the earlier they are made aware of online issues, the better.

As well as health visitors, GP surgeries are useful for disseminating information and we are looking at the best ways of providing e-safety material in those surgeries.

We have only just begun thinking about the possibilities that health services provide us for disseminating information and furthering our safeguarding work, but it is clear that they will be another vital plank in our strategy.

The third sector

Third sector groups can be invaluable in enabling access to a wider selection of the local community. Such groups can, for example, be communication channels to disseminate information about e-safety.

Our first contact with these groups came at Brent's Respect Festival, a yearly festival in Roundwood Park. There we ran a stall to promote e-safety awareness. This led us to establish links with some of the voluntary groups who were also there on the day – such as the Asian Women's Resource Centre and Brent Neighbourhood Watch Association. As a result of this meeting, we used the Asian Women's Resource Centre's summer school to pilot the Thinkuknow materials.

While chance contacts made at the festival and elsewhere have been invaluable, in order to have a more structured approach to community engagement we brought one of the three local neighbourhood co-ordinators on to the sub-committee. Neighbourhood co-ordinators manage community activities through local authority services, such as the extended schools network, adult education services and libraries, and the third sector. Having a neighbourhood co-ordinator on board has allowed us to join up our work with the schools with other activities to ensure that we are giving out a consistent message. It has meant, for example, that we can tie adult ICT education programmes into school-based campaigns aimed at parents.

Raising awareness of e-safety issues among the people who live in your area must be the cornerstone of any strategy.

Youth

Children and young people must be recognised as the experts in how they are using the internet; and their contribution to policy and strategy can be invaluable. In order to get a better idea of what they think about the risks and what we should be doing to help safeguard them online, we contacted our Youth Parliament.

Brent's Youth Parliament is made up of around 50 children and young people representing schools, voluntary organisations, youth organisations and special interest groups from across the borough. It sits once a month and this year has focused on the three areas which it identified as being most important to address – health and wellbeing, crime and safety, and sport and leisure. Within these categories, online safety was identified by the young people themselves as a key issue.

We have therefore asked a member of the Youth Parliament who is involved in the 'crime and safety' task group to join our e-safety sub-committee. We hope that this will be far more than a token gesture and that they will help us steer our strategy in the right direction. They might, for example, begin by canvassing opinion among representative groups or taking our policy ideas back to the Youth Parliament for review. Above all, we hope that the Youth Parliament will be genuinely involved in our decision making and help to shed light on areas we may not have even considered.

Crime and justice

While some of the most important work that we have undertaken aims to be preventative, it is a sad fact that we also need to react to internet crime as it happens. As a result we need clear lines of reporting between social care and the police to respond to incidents of ICT-related child abuse. A detective inspector from our police child abuse investigation team therefore sits on the e-safety sub-committee. With him we are working on procedures for joint working in these cases.

Where children are in a home, domestic violence is a child protection issue and can constitute significant harm. We have therefore engaged with the local domestic violence forum to explore possible links between ICT and domestic violence, such as the use of text messages to harass and intimidate, and links between abusive images of adults and child protection.

We have also already forged links with the community safety unit and will be looking at how we can take forward e-safety awareness within its programmes.

Actions to date

The following chronology details the actions taken so far by the Brent e-safety sub-committee.

Date	Event
December 2005	Agreed that e-safety should be embedded in the Children and Families ICT strategy and commenced work on this.
February 2006	Attended Becta e-safety conference.
4 April 2006	Initial presentation to the LSCB on e-safety. The Head of Systems and Performance Management was nominated as the LSCB e-safety lead.
10 April 2006	Attended the launch of CEOP – subsequently contacted CEOP to arrange a meeting.
5 May 2006	First meeting of the e-safety sub-committee – group met monthly thereafter.
9 June 2006	Visited CEOP for the first time and saw the Thinkuknow materials. Following this, invited representatives to present at Brent LSCB.
15 June 2006	E-safety presentation to Brent ICT subject leaders.
28 June 2006	Attended Capita conference 'Child protection on the internet'.

Date	Event
5 July 2006	Informal contact made with former colleague (now an ICT teacher) to get a better insight into pupils' understanding of e-safety.
16 July 2006	At Brent's Respect festival we ran a stall, using materials from CEOP's Thinkuknow campaign, to raise awareness with parents, children, young people and the public. Public interest in the subject was overwhelming. This day also led to us establishing links with some voluntary groups.
19 July 2006	Attended CEOP social networking workshops.
24 and 25 July 2006	All members of the group attended CEOP Thinkuknow training.
1 August 2006	Representative from CEOP presented to Brent LSCB to reinforce our message and introduce Thinkuknow.
14 August 2006	Thinkuknow piloted at the Asian Women's Resource Centre with a group of 15 young people.
18 September 2006	Meeting with London Grid for Learning to discuss presenting at the Brent Headteachers' ICT Conference. It was agreed that this would take place at CEOP with a strong emphasis on e-safety.
20 September 2006	Attended official launch of Thinkuknow.
19 October 2006	Visited Alperton High School at their request to discuss Thinkuknow and e-safety in general.
20 October 2006	Piloted Thinkuknow with 30 Year 9 pupils at Preston Manor City Learning Centre.
23 October to 6 November 2006	Thinkuknow presented to 150 Year 9 pupils.
24 October 2006	Attended IWF 10th Anniversary Roadshow.
1 November 2006	Brent Headteachers' ICT Conference held at CEOP. Presentations from Brent e-safety sub-committee and CEOP. This was a key point in getting Brent schools on board with the overall e-safety agenda. Headteachers were positive about rolling out Thinkuknow in Brent schools.

Date	Event
20 November 2006	Visited Woodfield School, a special school for pupils with disabilities, to meet teachers to discuss appropriate use of Thinkuknow with disabled children.
4 December 2006	Presented to a group of parents at Malorees Junior School.
December 2006	Letter sent to all schools in Brent offering training to representatives in Thinkuknow.
January 2007	Article placed in school governors' spring report to raise awareness among governors.
6 February 2007	E-safety group formally adopted as an official LSCB sub-committee.
April/May 2007	E-safety presentations delivered at parents' evenings in three Brent schools.
24 May 2007	First Thinkuknow training session run for teachers.
June 2007	E-safety public information advertisement for community station Life FM commissioned as part of series about 'risky behaviours'.

Local authority case study 2

London Borough of Havering

Penny Patterson from the Havering school improvement team of Havering Inspection and Advisory Service (HIAS), outlines her involvement in developing an e-safety agenda in the London Borough of Havering. Penny is also seconded to the London Grid for Learning (LGfL) as a key lead officer in the London Learning through ICT (L2ICT) project.

This is a snapshot of progress to Spring 2007, with much work continuing since then.

An overview of the borough

Havering is the most north-eastern of the London boroughs, located where the capital borders the green belt of Essex. Situated north of the Thames, it has a three-mile river frontage, and although geographically it is the third largest of 33 London boroughs, it has only the 14th largest population. Nearly 2,000 acres are farmland and parkland. The main towns are Romford, Hornchurch, Upminster and Rainham.

Havering's current population is about a quarter of a million, with 14 per cent of the population aged under 16 years. The population is predominantly white. The proportion of residents from black and minority ethnic groups is small at just under 5 per cent, although increasing. The total school population has remained stable at just under 40,000.

On the Indices of Deprivation 2000, Havering ranks at 214 out of 354. While overall it is quite a prosperous borough, there are areas of deprivation. Two wards show a high level of deprivation when compared with other wards across the country.

Safeguarding in Havering

Havering is generally a safe borough for children and young people to live.

The joint area review (JAR) identified that general safeguarding measures in Havering have been good. The organisation of safeguarding bodies is traditional, although since early 2006 full children's services and cross-service working has been in place.

Prior to the JAR in 2006 the issue of e-safety was underdeveloped and, while improving, was still not fully embedded in the work of the LSCB and council colleagues outside the school improvement service.

The challenges in raising e-safety across the council

Predating *Every child matters*, in 2002 Havering had a community safety group which included colleagues from education, social services, police and community safety. Several e-safety issues were raised through this group, including:

- Young people taking ill-advised photographs of themselves, unaware that their images could be construed as provocative. Distribution of photographs among friends was also an issue; some photographs were posted on websites, without permission, when friends fell out with each other
- A teacher uncovered homophobic bullying on websites. The young person targeted had been the subject of online polls inviting pupils to vote on how much they hated her. None of this web activity had been developed in school, but using the LGfL logs we were able to identify the three schools in Havering that had young people involved in this systematic bullying
- Pupils passing unsuitable materials between themselves and across schools on USB memory sticks.

How did we address this?

In response to such issues, the group issued Childnet leaflets to all pupils and parents through schools. In hindsight, we realised that we were unable to monitor the impact of this action, and using commercial leaflets had been costly.

The community safety group and associated e-safety activity did not continue. Issues were taken forward in education, but cross-service working did not carry on. At that stage the widening risks associated with digital technologies was not appreciated. Adults had limited understanding about e-safety issues and it was not flagged as a corporate issue at this stage. The approach to the issues was action planning based on specific incidents; the need for cross-service professional development on the topic was not identified. Unlike young people, who were already taking forward social networking and digital communication, adults viewed the problem as a rare occurrence or a 'fad'. Lack of understanding of the issues meant that, at that time, colleagues in the borough did not see the future implications of digital technologies for child safety.

Much of our e-safety approach has therefore developed in schools. Schools have had acceptable-use policies since the early days of the NGfL, initially based on model policies developed by Becta and Kent Education Authority. We are fortunate in that our headteachers understand some of the issues facing young people using digital technologies and, equally, the possibilities that digital technologies bring.

An annual residential conference for headteachers in 2004 focused on digital technologies. The American educator Alan November spent two days with heads, taking them through the issues of information literacy and what the

internet means to young people in terms of information, publishing and audience. This was a real 'penny drop' moment. Heads stopped thinking about the internet and its dangers from an adult perspective and saw the opportunities more clearly from a young person's viewpoint. At this stage the safety messages concentrated primarily on 'author, purpose and intent', and the range and validity of information.

Around this time, the Havering Inspection and Advisory Service (HIAS) ICT team began developing information literacy materials, and used these to work with colleagues, subject leaders at Key Stages 3 and 4, and some pilot pupil groups. These materials focused on the internet as an information source, and looked at bias and misrepresentation – separating fact from fiction. The problem was the naive trust that young people bring to digital technologies: it is this same naivety that leads them into risky situations with digital technologies.

Following the Becta national conference in February 2006, we realised that our teaching materials were out of date. The conference focused on the ECM agenda and the need for e-safety messages to have a wider audience. As part of my secondment to the London Learning through ICT (L2ICT) team, I brought together a group of colleagues from across the London boroughs to update LGfL e-safety materials and add to the policy and guidance materials we had historically been using. We were aware that many boroughs were facing the same challenge – a lack of resource – and, working together, we were able to begin putting together a set of materials for schools, teachers, pupils, parents and LAs.

The development group represented five of the 33 London boroughs (Havering, Islington, Barnet, Kensington & Chelsea and Brent). LA colleagues worked voluntarily and, through the L2ICT project, one group member was funded for six days to co-ordinate the work. The result was substantial policy, information, training and guidance materials which are now available in the safety section of the LGfL website [**http://safety.lgfl.net**]. All materials are open access and have been publicised through other grids and national organisations such as Naace [**http://www.naace.co.uk**]. This policy guidance is constantly under review and recent changes have introduced more specific references to social networking and cyberbullying guidance and an extended staff acceptable-use policy.

Two members of the Havering school improvement team gained individual accreditation as CEOP Thinkuknow trainers as soon as the scheme was launched in summer 2006. This is being rolled out to schools and the materials have been delivered to school improvement team colleagues.

Awareness raising – schools

Over time, schools have begun to acknowledge their role in e-safety.

Primary schools, in particular, have been proactive in seeking support from the school improvement team. Prior to the availability of CEOP materials, we developed home-grown parents' sessions which have been delivered to about 15 per cent of primary schools.

Secondary schools have been slower to develop their role. Initially the problems were viewed as primarily home-based issues. Information sessions to raise awareness have been delivered on a number of occasions within the LA at heads briefings, security conferences and ICT conferences. Finding ways of supporting colleagues in senior management teams in secondary schools is key to reaching the pupils. One secondary school that has fully embraced e-safety issues used the Becta SRF (self-review framework) as part of its ICT Mark accreditation – the whole-school view of ICT being led by the senior management team, not by the ICT department. This focus on ICT across the school extends across and beyond curriculum boundaries to take on wider issues such as e-safety. Parent briefings in this school were very well attended, with two evening sessions attracting more than 100 parents to each. The significant feature in this school is the role of ICT co-ordinator being separate from that of ICT subject leader. The ICT co-ordinator is the assistant headteacher and collective responsibility for cross-curricular messages is well developed.

A new route to raising awareness within Havering is through the school governing body. At an optional e-safety training session for governors, 10 per cent of schools were represented. Half of those attending took the information straight back to school, and the headteachers of those schools subsequently organised parent and staff briefings. This governor briefing model is being repeated. Some governing bodies have also added e-safety reporting as a standard agenda item. Statutory racial incident monitoring is followed by e-safety; in some schools the reporting is under the five ECM headings which include 'staying safe'.

Awareness raising – the LSCB

Finding the opportunity to introduce e-safety to other colleagues in the borough has been harder. Local guidance and also inspections (such as the JAR) have not mentioned ICT or e-safety, although this is now altering with additions to the SEF (self-evaluation framework) used by schools, which now has specific references to ICT and e-safety. We recognised that until national guidance and monitoring is introduced for a topic, there is often insufficient time and resource to develop content within a local authority. The schools agenda was led by CEOP, Becta and the London Grid for Learning materials, but there was nothing similar for other children's services colleagues.

In Havering, we provided JAR inspectors with information on e-safety issues. The JAR process is lengthy and key foci for the inspection and visits by inspectors are available well in advance. This gives LAs an opportunity to present their key messages as part of these foci even when not specifically asked for.

Although there is a concentration on actual harm to children in the local area, the virtual environment is often misunderstood and there has been a lack of information about the issues and implications of e-safety. Until the formation of CEOP, media coverage was not extensive and focused on extreme cases only. CEOP has done much to alter the media profile of e-safety risks and issues and this, in turn, is helping colleagues to understand digital technologies. Before CEOP existed we had an adult who failed to see a risk in a known paedophile's daughter having a PC and webcam in her bedroom; luckily this analysis of risk has shifted substantially.

The full LSCB had a presentation on e-safety, the Becta e-safety publication for LSCBs was issued, and members of the group were shown the kinds of activity young people are involved in. This was followed up with presentations to services staff, foster carers and youth services. Where possible we are trying to ensure that these presentations can be cascaded across teams. The training load for this topic is more substantial than for other digital technology issues. The training materials we have developed are only a part of the presentations we give: much of the content is anecdotal scenarios which help colleagues to develop empathy and understanding of the environments, risks and issues.

The school improvement team has taken the lead on e-safety purely because we had experience of the issues before LSCB colleagues. The fact that we had also tried new digital technologies meant that we had a greater insight into the risks. The presentations we have given on risks, issues and benefits to adult groups often have a shock factor. Adult groups are not aware of the activities young people are engaged in; the amazement is evident time after time, and it is interesting to observe adult responses. Before awareness raising, the view often underplays the e-safety issue as 'it's something young people do'. Following awareness raising, adults often overestimate the risks, forgetting that many e-safety situations are solved by young people and their peer groups; adult intervention is not needed for every situation. Longer reflection is followed by a more balanced approach, acknowledging that virtually every youngster is faced with situations which could be a risk unless handled sensibly. Most youngsters take the safe route. Research has identified the youngsters that are likely to be at risk – youngsters who are less confident with technology and youngsters who have other problems are those that adults quickly identify. We are also looking at ways of promoting able, ICT-capable young people as a significant risk group, since because of their higher level of skill and confidence they may take more risks with digital technologies.

A training programme with opportunities for all council areas and wider groups has been set up with the LSCB. The opportunities have been carefully planned for different groups, but the key aim across the programme is increased understanding and a better assessment of e-safety risks.

Awareness raising – wider groups

Liaison with Havering police has been very positive. The partnership started in a drive to reduce burglaries, with the school improvement team providing very practical input to a significant burglary-reduction programme using forensic and etched equipment marking. Police participation was to DI level and the chief inspector also attended a schools conference. Shortly after this, Havering police set up HJAG (Havering Joint Action Group) – a cross-council action group led by the police but drawing in colleagues from across the council. The security partnership was held up as an example of strong networking that the police wished to replicate across the borough, and HJAG has subsequently provided links with further services such as the DAAT (Drugs and Alcohol Action Team). We now have an ongoing forum to raise issues and concerns which can include child safety issues.

Monitoring and reporting

The LGfL broadband service has given us new reporting opportunities. Following the homophobic bullying incident (described earlier) we were able to get a full report across all Havering schools on the bullying websites which contributed to this case. Likewise, when community safety and the police wanted to investigate social networking sites containing 'ill-advised' content, we used similar reporting to establish the extent of access, and to identify whether sites were being created or visited in school. LGfL reporting helped us to establish that this was primarily an 'at home' problem, but that attempts were being made to view the sites in school. It also provided school-by-school data showing access date and time and the computers where access was attempted. This, linked to teacher information about class seating plans, identified the young people involved.

This link between education, the police and community safety existed because long-term staff had built up an *ad hoc* colleague network. Wider council understanding of the reporting and security features offered by LGfL in schools was not known. This is likely to be a common issue across London boroughs. LGfL works hard to publicise the collegiate and consortium aspects of the grid, but outside education – and specifically within corporate ICT in some boroughs – LGfL is mistaken for an external commercial company.

The reporting statistics available across LGfL include individual URL access by time, school and IP address. Every request made through the URL filtering service is logged, including date and time, IP address, URL details, category of the URL and

whether it was blocked or allowed. All logs are kept for a minimum of three months and are fully searchable. They are stored, for forensic purposes, unprocessed.

This gives the opportunity to identify the logged-on individual, but it requires additional school network and teacher information to substantiate who was actually sitting at a computer in class. We have two schools with an additional in-school proxy and firewall. Because of this, the whole school sits behind a single public-facing IP address which then relies on in-school security reporting to identify specific PCs. We have additionally shared knowledge of this reporting availability with union colleagues in case situations should arise where evidence of internet access and activity should be needed.

In London this reporting is now available directly to schools. An online wizard allows selection of items such as URL, time slot and IP range. Reports which cover a time period longer than a few hours may need to be run overnight. Results can be delivered in spreadsheet and other formats to a school email address.

The reporting facilities have been a useful tool for schools in working with parents; it has helped to dispel concerns about access to unsuitable materials. No filtering system is perfect, but filtering breaches have been very rare, and full details have been available quickly to schools to share with the families concerned. The speed at which an accurate report can be run helps to avoid speculation and anxiety.

Plans for the future – the current challenge

We recognise the continuing need to keep colleagues across all areas of the council informed about e-safety.

In developing an awareness of e-safety, the LSCB went through a series of stages:

- There was a lack of awareness of e-safety as an issue.
- Initially the school improvement team provided support for e-safety.
- The school improvement team worked with the LSCB to increase personal understanding, empowering them to take corporate responsibility.
- The LSCB is now making active use of the school improvement team to provide professional development for groups across children's services.

Based on our experiences to date, plans to further develop the e-safety agenda in Havering include:

- Rolling out Thinkuknow beyond pilot schools, specifically targeting secondary schools (50 per cent by April 2008) and Year 6 in primary schools
- Gaining acknowledgement of the 'corporate parent' role, continuing to work with social services, and offering wider professional development sessions to colleagues across the council

- Getting colleagues to reflect on their views on the risks presented by e-safety – many underestimate/do not recognise the risk, but with understanding comes an initial tendency to overestimate the risks; then, with time and reflection, a balanced view of the risk
- Having the LSCB increase awareness of issues with colleagues across children's services and other service areas
- Getting the LSCB to look at engaging community groups to spread the e-safety messages
- Appointing an e-safety officer on the LSCB
- Having a wider conversation across the authority on e-safety risks.

Advice for other local authorities

- Don't view this as an ICT issue, don't allow technology to obscure your view of the real issues of child safety with digital technology and don't delegate responsibility to technical or ICT colleagues.
- Talk to young people in your local area to keep informed about emerging new technologies.
- Be aware of local trends – certain games and social networking sites take hold in specific areas.
- Be aware of the 'tipping point' factor – use an acquaintance builder to help spread the message and link together the groups across children's services, the wider council and extended partners.

Local authority case study 3

E-safety in Kent

In Kent, an e-safety officer was appointed in January 2006 to develop and drive e-safety activity across the county. This report provides a snapshot account of their activity during the first 15 months of their appointment, to April 2007.

The Kent context

Kent is the largest local authority in England, serving a population of 1.3 million. It has a mixture of rural and urban areas, affluence and deprivation and a varied pattern of twenty large- and medium-sized towns, many small towns and villages and no dominant town or city.

Kent's socio-economic profile is unlike the rest of the South East. While there are areas of prosperity in Kent, overall there is low employment growth, low household income and high deprivation compared to the rest of the region. The coastal areas in the north and east have suffered the most, with the demise of their manufacturing industries, the loss of the Kent coalfields, and the decline of their tourist industry. While the coastal areas are by far the worst affected, deprivation is also significant in areas of Ashford and Canterbury. Even in the more prosperous areas of Kent, pockets of significant deprivation exist at ward and neighbourhood levels.

In other parts of Kent, a buoyant local economy means that the cost of living, wages and property costs are all growing quickly. This leads to significant pressures. Overall the county's average index of multiple deprivation is among the highest of the 11 LEAs identified by Ofsted as statistical neighbours. Fewer Kent residents have higher education qualifications compared to statistical neighbours.

The economic and social polarisation within the county has an impact on educational achievement. Children living in poverty have low achievement levels and schools serving disadvantaged areas strive to raise standards in very challenging circumstances. While attainment levels show that many of our schools already perform well, there are also many that need continued support and assistance to improve.

To address these challenges and to raise standards in all our schools, a number of major changes and strategic developments have been initiated over the last two years. Principal among these has been the 'best value review' of school improvement. This led to two major developments: the creation of local clusters with resources devolved to them to promote collaborative approaches to school improvement; and the restructuring of the education department to bring a more focused approach to raising standards and safeguarding children and young people.

Local strategies for e-safety

Kent County Council appointed an e-safety officer in January 2006 in light of the creation of the Children, Families and Education (CFE) directorate and a recommendation in the Becta document *E-safety – safeguarding children in a digital world*:

> 'That directors of children's services for each local authority nominate a single point of contact within the authority to lead on e-safety work. Urgent attention should be given to ensure that every local authority meets its requirements under the *Every child matters* programme…'

While Becta had identified some key areas of focus, it was also necessary to identify areas where e-safety issues needed addressing in Kent specifically. These included:

- schools (primary, secondary, SEN – student, teacher and governor training)
- youth centres
- pupil referral units
- health needs education service (previously known as hospital schools)
- other non-education areas including:
  - social services
  - children's safeguards service
  - parents and the community
  - libraries
  - additional services providing internet access to young people.

E-safety role and responsibilities

The key roles and responsibilities of the E-safety Officer were identified upon their appointment and have provided a template to create an action plan for their activities. They are as follows:

- Supporting the national e-safety strategy
- Liaising with national and international organisations (CEOP, Becta and Virtual Global Taskforce)
- Creation and management of a multi-agency e-safety board
- Creating a dynamic and immediate online communications channel that communicates and raises awareness of e-safety issues with schools and LA stakeholders (blogs, online resources)
- Developing collaborative multi-agency policies and approaches for online safety
- Assessing risks of new and emerging technologies and communicating these to stakeholders
- Providing training and supporting resources to schools
- Providing an information point on e-safety issues
- Handling press enquiries and requests for information.

E-safety activities in 2006

The E-safety Officer spent their first year in post actively working to raise awareness of e-safety around the county, including identifying approaches to highlighting e-safety to the identified groups and initiating an education programme for secondary schools. The following information is a review of the work that the E-safety Officer was involved in during this time.

Research

Initially, the E-safety Officer spent the majority of their time researching e-safety and improving their knowledge of technology and the risks associated with these technologies. A steep learning curve was necessary to ensure that they were fully briefed and aware of the e-safety issues that affect our children and young people. During the research process, a number of organisations and charities were identified that were already creating materials and providing advice and guidance about e-safety. To keep a record of all of the websites and also to record details of e-safety-related news reports and documents sourced, an 'e-safety in schools' blog was created [**http://clusterweb.org.uk?esafetyblog**].

The blog contains links to useful information categorised for students, parents and teachers and also links to useful e-safety documents, reports and leaflets. News items are regularly posted on the blog reporting on issues raised in the press, highlighting useful resources and promoting the work that the E-safety Officer has been engaging in. Some people have posted comments to the blog and comments have been received that it is a very useful source of information.

Training

In April 2006, the Child Exploitation and Online Protection (CEOP) Centre was launched by the Home Office to vigorously pursue criminals and to help children and young people become more aware of online dangers.

The E-safety Officer contacted CEOP and arranged a meeting to discuss how Kent could become involved with their work and convey their national message locally. As a result of this meeting, Kent became the first local authority to pilot CEOP's education programme for children and young people, Thinkuknow.

The Thinkuknow resources have been created as part of CEOP's harm-reduction strategy. These resources draw attention to what young people know about the risks they may encounter while using the internet. The programme uses three themes to focus on key messages:

- How to have fun online
- How to stay in control online
- How to report a problem online.

As part of this, CEOP has developed an interactive presentation, which it aims to deliver to all secondary-age children between the ages of 11 and 14. This is part of a package which includes films, leaflets, posters and a training pack for all child-protection professionals in the UK. The programme will eventually be rolled out to primary-age children as well [**http://www.thinkuknow.co.uk**].

The E-safety Officer organised a pilot of 15 secondary schools to receive the training and to feedback to CEOP through student and staff evaluations.

Also, the help of the Secondary Hands-on Support (HoS) Advisor for the Advisory Service Kent (ASK) was enlisted to provide support throughout the pilot and continue to be involved with future training.

A CEOP representative trained Kent's E-safety Officer and the Secondary HoS Advisor to use the Thinkuknow programme and they delivered the training sessions to the 15 pilot schools on behalf of CEOP.

The initial approach was to train selected members of staff from a variety of the schools' faculties, namely IT, pastoral (such as PSHE/Citizenship teachers and designated child protection co-ordinators) and senior management team members. Kent's E-safety Officer and the Secondary HoS Advisor then delivered one student session to provide the teachers with an opportunity to see how to deliver a session. The training is aimed at 11–14-year-olds but schools were encouraged to use the training package as a debate topic for older students and, in some cases, train their sixth-form peer mentors to deliver the training themselves. This widened the spectrum and meant that all students were involved in discussions about e-safety.

After the initial teacher training sessions, teachers were encouraged to devise an implementation plan for disseminating the training to students. This wasn't necessarily a detailed plan but rather a decision on how the training would be delivered in school, for example in dedicated lesson time (such as PSHE lessons), form/tutor time and focus days.

The pilot finished in December 2006 and was a great success. All schools involved said how impressed they were with the quality of the training and how important it was. As a result of this success, it was decided that training should be provided for all secondary schools in Kent. Due to resource and time constraints, it was not viable for the E-safety Officer to deliver the training to individual schools and therefore a cluster-based approach was devised.

Four cluster-based training sessions have already been organised and two sessions have already been delivered. These events have proved a great success. The E-safety Officer has attended 'hands-on support' meetings around the county to raise awareness of the cluster sessions, and a session for every cluster will be arranged. Each school is invited to send two or three representatives to the training.

One of the key evaluation points identified from the pilot training was that, while teachers felt comfortable delivering the training to students, they felt that they could not comfortably converse about the technology with students because they do not use it themselves. It was decided to include a 'tour of technology' in the cluster training session to give teachers the opportunity to try out sites like MSN, Bebo and MySpace and to identify the risks of these technologies.

The group are divided into small groups of two or three and asked to evaluate critically a specific technology. In doing so, they were asked to do the following:

1. **Identify the risks of the technology**
2. **Look at the content – Is it inappropriate? Can you even tell?**
3. **Decide how you could manage the risks.**

Allowing the teachers to use the technology themselves and identify the risks improved their confidence and they said they would now feel more comfortable discussing the technology with the students. At a few of the cluster sessions, the host school arranged for some of their sixth-form students to attend and this provided a great opportunity for the teachers to ask the students what technology they used and, more importantly, why they used it. A number of the teachers that were involved in the training couldn't understand why a young person would prefer to talk to their friend on MSN than phone them, or why they would want to create a Bebo or MySpace site. The students told the teachers why they used the technology and the teachers commented how useful that aspect of the training was. Also, while the students knew a lot about being safe online, they also reported that they had learnt a lot about online risks as a result of the training and would be speaking to their peers about what they had learnt.

This training has been very well received by schools who have taken part and it is important to consider provision to review schools' training on an annual basis. There is a need for schools to revisit e-safety training with their students every year and to update them on the risks of new technologies.

Consideration should be given to providing a similar training scheme for primary schools using the CEOP primary resources.

While schools provide the most obvious route to training students, there are a number of children and young people in Kent who do not attend mainstream school. These children are often identified as vulnerable and, as a result, are a key target group for receiving the Thinkuknow training.

The health needs education service (HNES) provides education for students not in school because of health reasons. The East Kent office expressed an interest in receiving the training, as their teachers often have 1:1 contact with pupils and could therefore deliver the training to students on an individual basis. Every member of staff was trained and training with students has started. Provision has been made to now deliver this training to the other area HNES offices.

The Sittingbourne Challenger Centre is a pupil referral unit (PRU) maintained by the local authority for children who are not able to attend a mainstream or special school. Its students are also identified as vulnerable. The centre contacted Kent's E-safety Officer and asked them to deliver the training to their students. Training provision for all pupil referral units is also now in progress.

Most school governors are involved in the creation and implementation of school policies and need to be kept abreast of any issues that affect their students. The E-safety Officer suggested that governors need awareness of e-safety and the training that is being offered to secondary schools. After a number of meetings with the Governor Training Department, the E-safety Officer teamed up with the eGovernment and Communications Manager to deliver a joint training session for governors. The governor training sessions were scheduled for January–May 2007 and information about e-safety has also been included in the governors' newsletter. Provision should be made to review training for governors on an annual basis.

As part of the reorganisation at Kent County Council, children's social services are now part of the CFE Directorate. The E-safety Officer met with one of the managers in children's social services who was, at that time, purchasing computers for foster carers to have in their homes. The internet safety information that they were providing was quite outdated and did not include many of the technologies that children and young people use today. As a result the E-safety Officer suggested that they update their information and provided them with some resources to do this. Consideration should be given to identifying training needs of foster carers and adoptive parents.

Youth centres were identified as a key environment where children and young people access the internet, and it was decided that youth workers would also benefit from the Thinkuknow training. It is important to educate youth workers about online risks and how to minimise them, so that they can then pass this information onto the children and young people that attend the youth centres. The E-safety Officer trained two districts, and training is ongoing. This should also be reviewed on an annual basis in light of emerging technologies.

Raising awareness

Raising awareness around the county was identified as a key activity of the E-safety Officer's agenda for 2006. As a result, the E-safety Officer attended a number of meetings, briefings and conferences to talk about e-safety, as briefly detailed below.

The CEOP videos and Thinkuknow presentation were shown at the ICT Officers meeting. The ICT Officers group comprises officers from a variety of areas in the Children, Families and Education Directorate. All are involved with ICT in education. The Director of Resources for Children, Families and Education

expressed full support for this campaign and suggested that the E-safety Officer attend a senior management team meeting to raise awareness with senior managers in the directorate.

The E-safety Officer therefore attended a SMT meeting and showed the CEOP videos and Thinkuknow presentation. The need to address e-safety issues in schools was highlighted and it was suggested the Thinkuknow programme be used as a training resource in schools. The Director of Children, Families and Education gave his full support and continues to support this initiative wholeheartedly.

The E-safety Officer also attended a number of headteacher briefings around the county to raise awareness of the Thinkuknow training, and attended the Headteachers ICT Strategy Group meeting to discuss e-safety and engagement of headteachers.

The Local Safeguarding Children Board (LSCB) has been mandated to address the issues of e-safety. As a result, the E-safety Officer attended an LSCB meeting to highlight the work that had already been initiated and to discuss future plans for raising awareness and educating children and young people about e-safety in 2007. Provision should be made to attend regional safeguarding children board meetings to discuss future plans for e-safety with local areas.

An e-safety conference was organised to raise awareness with Kent schools, KCC officers and advisors. Representatives from both Becta and CEOP were invited to speak about e-safety on a national level. An officer from Kent Police presented his experiences of investigating online crime, and KCC officers gave presentations about e-safety on a local level.

Collaboration

As previously mentioned, Kent's E-safety Officer has worked with officers from education, social services, youth and health. The intention is to get everybody working together with the aim of ensuring that Kent children and young people are safe online. This can only be achieved if everyone is briefed and aware of the e-safety work that has taken place and is planned for the future.

An e-safety strategy group was set up by Kent's ICT Projects Manager, with the initial task of re-writing the schools internet policy to provide schools with a template to develop their own policy for the use of the internet and electronic communications.

Kent County Council has produced internet policy guidance for Kent schools for the past eight years. It was decided that the document needed a wider remit that would cover e-safety. This included incorporating information about mobile phones, wireless devices and also information about the technology that children and young people are regularly using (for example social networking

sites and instant messaging). The document also needed to include child protection information and advice for staff about how to respond to an online incident of concern.

The Kent e-safety strategy group revised and revamped the Kent schools' internet policy. Renamed 'Schools e-safety policy guidance', the document was launched at the e-safety conference in March 2007. Kent's E-safety Officer was heavily involved in the re-writing process and also contributed a great deal to the new sections and amendments. This document is the work of a collaborative group with a variety of expertise and it is hoped that it proves a valuable tool for schools in ensuring they are e-safety aware and have taken the necessary precautions to safeguard their students. Consideration should be given to the work of the e-safety strategy group and how they can contribute to the wider e-safety agenda in the future.

The e-safety strategy group includes a variety of KCC and external representatives who are all involved in the safeguarding and education of children and young people. Group members include:

- E-safety Officer
- ICT Projects Manager
- Training and Development Manager, Children's Safeguard Service
- Primary ICT Advisor, ASK
- Technical and Filtering Officer
- Special Educational Needs ICT Manager
- Director of eLearning, Kent Grammar School
- Network Manager, Kent Grammar School
- Kent Police, Force Youth Crime Reduction Officer.

The group is an example of how multi-agency collaboration is essential to ensure a co-ordinated and effective approach to managing e-safety in Kent.

Kent's E-safety Officer has also worked closely with the Children's Safeguard Service to develop a co-ordinated approach to e-safety.

Both the E-safety Officer and the Children's Safeguard Service Training and Development Manager have delivered internet safety training to Kent teachers to raise awareness of e-safety issues around the county.

The Children's Safeguard Service considers e-safety in two broad areas:

1. Protecting children from harm
2. Safe practice for staff and children.

In the last year, the Children's Safeguard Service has received a number of reports relating to these areas of e-safety. They include:

- Sexual assault following online grooming in an instant messaging site
- Making and distributing indecent images following online grooming and threats
- Threats of violence and racial abuse via text messages and email
- Members of staff accessing pornography on school equipment (including on school premises and in school time)
- Incitement to harm other children published on social networking sites
- Children with indecent screen savers on their mobile phones
- Derogatory comments about staff and pupils published on social networking sites (such as **RateMyTeachers.co.uk**).

The reports highlight that e-safety issues are occurring in schools, and that staff and children need to know how to deal with them from both an educational and child-protection view. It is therefore vital that the Children's Safeguard Service continue to work with the E-safety Officer to develop a co-ordinated approach to e-safety.

The E-safety Officer has attended a number of child protection training sessions around the county with the Training and Development Manager. The child protection training often includes information about e-safety and dealing with children's reports of online abuse. The E-safety Officer has also attended safeguarding days to present the Thinkuknow programme and discuss what Kent County Council is doing to safeguard children and young people online.

Kent Police sees e-safety as an important issue and has dealt with many cases of internet grooming and incidents of misuse in the past. As a result, Kent Police has teamed up with Kent Children, Families and Education Directorate to work together to raise awareness and educate children and young people of the risks online.

Kent Police supports CEOP's internet safety training programme and the team of Youth Crime Reduction Officers who work in and with schools and youth groups have been trained as part of the initiative.

A representative from Kent Police is also a member of Kent's e-safety strategy group.

Summary of e-safety work in 2006

Since 2006, the profile of e-safety has been raised dramatically on a national basis by organisations such as Becta and CEOP. Through the work of Kent's E-safety Officer, the e-safety strategy group and individual officers, this has been mirrored on a local basis. Raising awareness of the dangers that children and young people can come into contact with online is vitally important to ensure that children are safeguarded from online abuse, bullying and viewing inappropriate content.

During 2006, Kent's E-safety Officer raised the profile of e-safety and initiated a number of activities aimed at protecting our children and young people online. It is important to identify constantly emerging technologies and their perceived risks to children and young people, and to educate all parties who work with children about the online risks and measures needed for safeguarding.

Lessons learned in 2006

Through the e-safety work conducted in 2006, a number of lessons were learned.

- Collaboration is vital – in order to achieve a successful approach to raising awareness and educating children, young people, teachers, officers, advisors and parents, it is important for all parties involved with these groups to work together in a co-ordinated approach. Without collaboration, a number of e-safety activities would not have been as successful as they were, and their impact would have been reduced.
- Raising awareness is very important – in order to raise the profile of e-safety and provide education for children and young people, raising awareness is key. It is vital to highlight the key issues and identify approaches for addressing these issues. If people are not aware of the issues, it is often difficult to get their full support and progress can be hampered.
- Engage headteachers and senior leaders – in order to achieve full support and commitment, it is important to engage those people who control decisions and can make an impact. In some cases, senior leaders and headteachers were not aware of e-safety and the activities surrounding it. As a result it was often difficult to engage them in the training or to even get the message across to staff. By working with and gaining the full support of headteachers and senior leaders, it is often easier to engage other staff and students.

Activities for 2007

It has been decided that Kent requires an e-safety strategy to determine activities that the E-safety Officer should be involved in and to identify key areas to focus on. The e-safety strategy will be formed on the basis of the work that the E-safety Officer was involved in during 2006 and the activities of 2007. The following statements provide information about the activities the E-safety Officer has been involved in during the first quarter of 2007, and how they will contribute to the e-safety strategy for Kent.

The Anti-bullying Strategy Group asked the E-safety Officer to join the group to provide advice and guidance about cyber-bullying and measures that can be taken to raise awareness of cyber-bullying tactics and ways to safeguard against these. It has been suggested that the E-safety Officer should also play a part in developing the anti-bullying strategy for Kent.

The E-safety Officer attended two area safeguarding board meetings to show the Thinkuknow presentation to child-protection professionals and to discuss ways to widen the arena for raising awareness of e-safety. One group has suggested work with Connexions and doctors' surgeries. Provision needs to be made in the strategy for identifying other areas outside of education that would benefit from e-safety advice and training.

Following the success of the initial e-safety conference, further conferences have been scheduled. The profile of e-safety has been dramatically raised in Kent and a number of schools are seeking guidance and advice. As a result of the conference, key areas for development in Kent are being identified, with a suggestion of a pilot for the primary training and the need to appoint a full-time e-safety officer for the CFE Directorate.

Kent's E-safety Officer was invited to attend training sessions for teachers returning to the profession to show the Thinkuknow training programme and to provide information about the popular technologies that young people are using, and the risks associated with these technologies. The first session was a success but showed that awareness of the technologies and their associated risks was low. This has highlighted the need to work closely with services offering initial teacher training and Inset to provide teachers with a wider understanding of the technologies that young people use, and an opportunity to identify the risks and ways to safeguard against them. This is an area for development.

As a result of the work that has been initiated with the CEOP, the E-safety Officer was invited to attend the DfES conference *Safeguarding children online: taking forward a strategy at local level*. The conference was aimed at LSCBs and the E-safety Officer was asked to present on the topic of implementing e-safety practices within a local authority. The aim of the presentation was to raise awareness within LSCBs of CEOP's education programme for the coming year and of the steps an LSCB can take to raise awareness, empower children and young people to take control to stay safe online and to share experiences across LSCBs about taking forward an e-safety strategy. A number of delegates asked questions about how Kent had started to address e-safety issues locally and commented on Kent's effective approach to raising awareness and providing e-safety education for our young people.

Due to the re-organisation at KCC and the development of the CFE Directorate, the E-safety Officer now has a remit to work with families on e-safety issues. A local school invited the E-safety Officer to lead a parents' evening on e-safety, and parents of students from both primary and secondary schools were present. The evening was dedicated to e-safety and provided parents with an opportunity to discuss popular technologies used by young people and to be made aware of risks and ways to safeguard against them. This has identified an area for discussion and, when developing the strategy for e-safety, approaches to engaging with parents should be considered.

Areas for future focus and development

The cluster training sessions for secondary schools will continue until the end of the academic year 2007. The e-safety strategy should consider provision for revisiting training for secondary schools to provide schools with an opportunity to highlight risks of new emerging technologies and to remind them of current online risks and ways to safeguard against them. Consideration should also be given to initiating a training scheme for primary schools. In addition, research should be initiated around offering a training package for students with special educational needs.

Collaboration between internal departments and external organisations is vital to continue the successful development of the e-safety agenda successfully, and the e-safety strategy should consider ways in which this can be achieved. It should also seek to identify other areas outside of education that would benefit from e-safety advice and training.

Engaging with parents should become a key focus area of the e-safety strategy and the opportunity to provide training sessions for parents should be considered. It is important to engage with as many parents as possible, so a multi-strategy approach should be considered.

Initial teacher training and training for teachers returning to the profession should include an element of e-safety training. It is important that these groups be made aware of online dangers and ways to safeguard against them. This area has already started to be addressed as a result of one training session for teachers returning to the profession. More work needs to be initiated to make contact with organisations that offer training to these groups in order to identify if there is any scope to include e-safety training as part of the overall training package.

Current packages to train students (such as Thinkuknow) should be amended to include more information about online risks other than child abuse and grooming. More focus should be given to areas including viruses, identity theft and accessing inappropriate content, as these are also dangers that young people can face on a regular basis online.

Looked-after children and those who support them should also be provided with e-safety advice and training. Training for foster carers and adoptive parents should be considered as a starting point and work initiated with this specific group to identify other key areas within children's services that would benefit from e-safety training.

Conclusion

The past year has seen the profile of e-safety rise dramatically through a number of national initiatives. Kent Children, Families and Education Directorate is committed to ensuring that e-safety is high on the agenda when considering the safeguarding of children and young people and as a result appointed an E-safety Officer to address these issues.

The ever-increasing student use of the internet and other communication technologies means that students are more likely to encounter dangers online. It is vital that we educate our students to the dangers of the internet and provide them with practical advice about how they can control their own online experiences.

While the school setting provides the most natural route to providing this additional education to children and young people, there are also a number of organisations that cater for those who, for a number of reasons, are not in mainstream school. These groups must also be identified and engaged to ensure that as many children and young people receive the e-safety advice they require.

Also, a number of groups who work with children and young people may also benefit from receiving e-safety training themselves, and it is important to engage with these groups to ensure that they are reiterating the e-safety messages to children and young people.

It is important to note that while there are dangers associated with the internet and other communication technologies, they provide fantastic tools for research, communication and entertainment. We must ensure that children and young people are not fearful of using technology, but rather appreciate the dangers and know how to protect themselves online.

Becta leading next generation learning

B

Example incident flowcharts

Chart 1: Kent County Council CFE Directorate
E-safety incident flowchart

Chart 2: Staffordshire County Council
E-safety incident flowchart

Chart 3: Northern Grid for Learning
Committing an illegal act – Did you know?

Chart 4: Northern Grid for Learning
What to do with suspicious email

LSCBs and their member agencies may wish to develop their own incident flowcharts, based on local circumstances.

Thanks to colleagues in these authorities for sharing these materials.

Chart 1

Kent County Council CFE Directorate E-safety incident flowchart

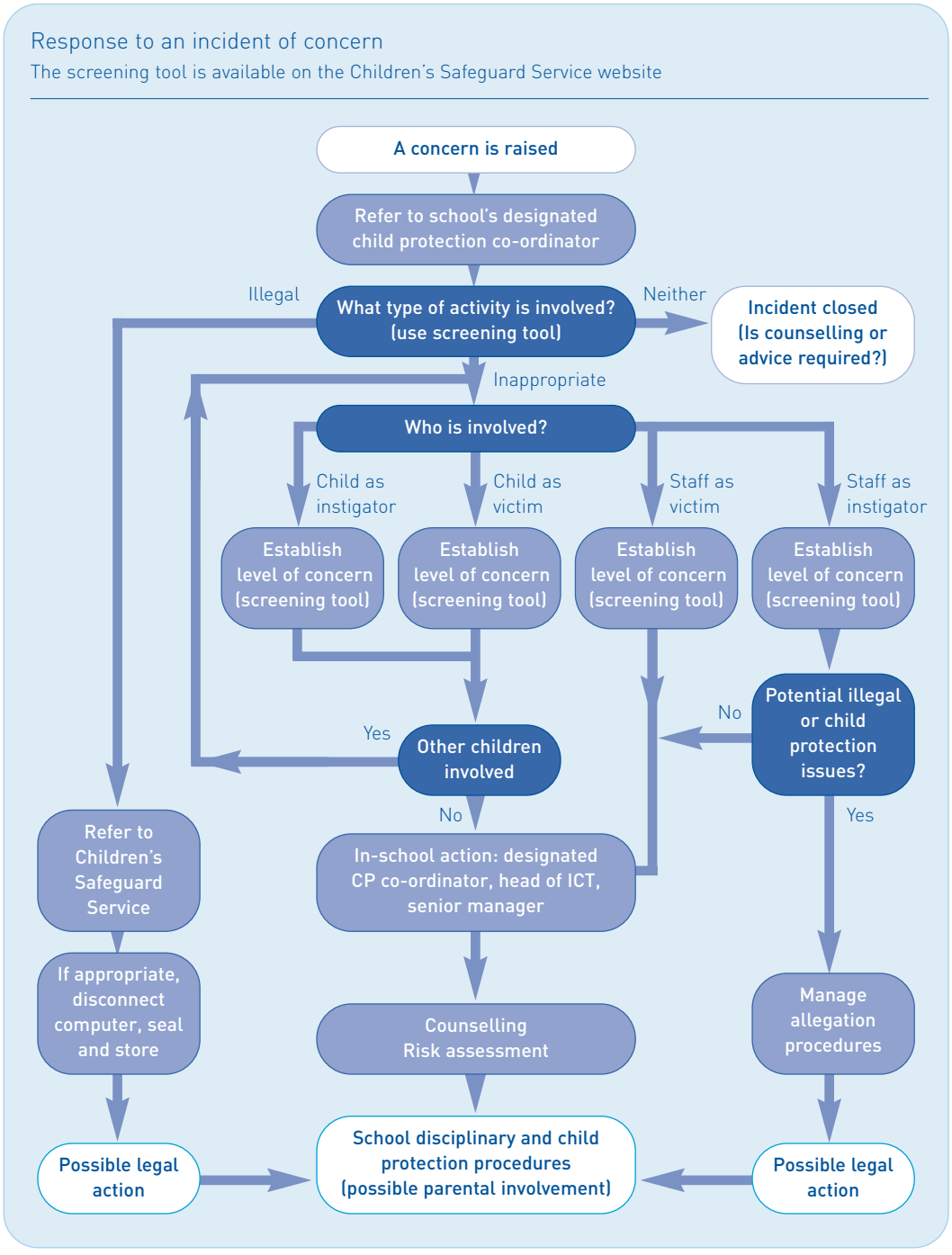
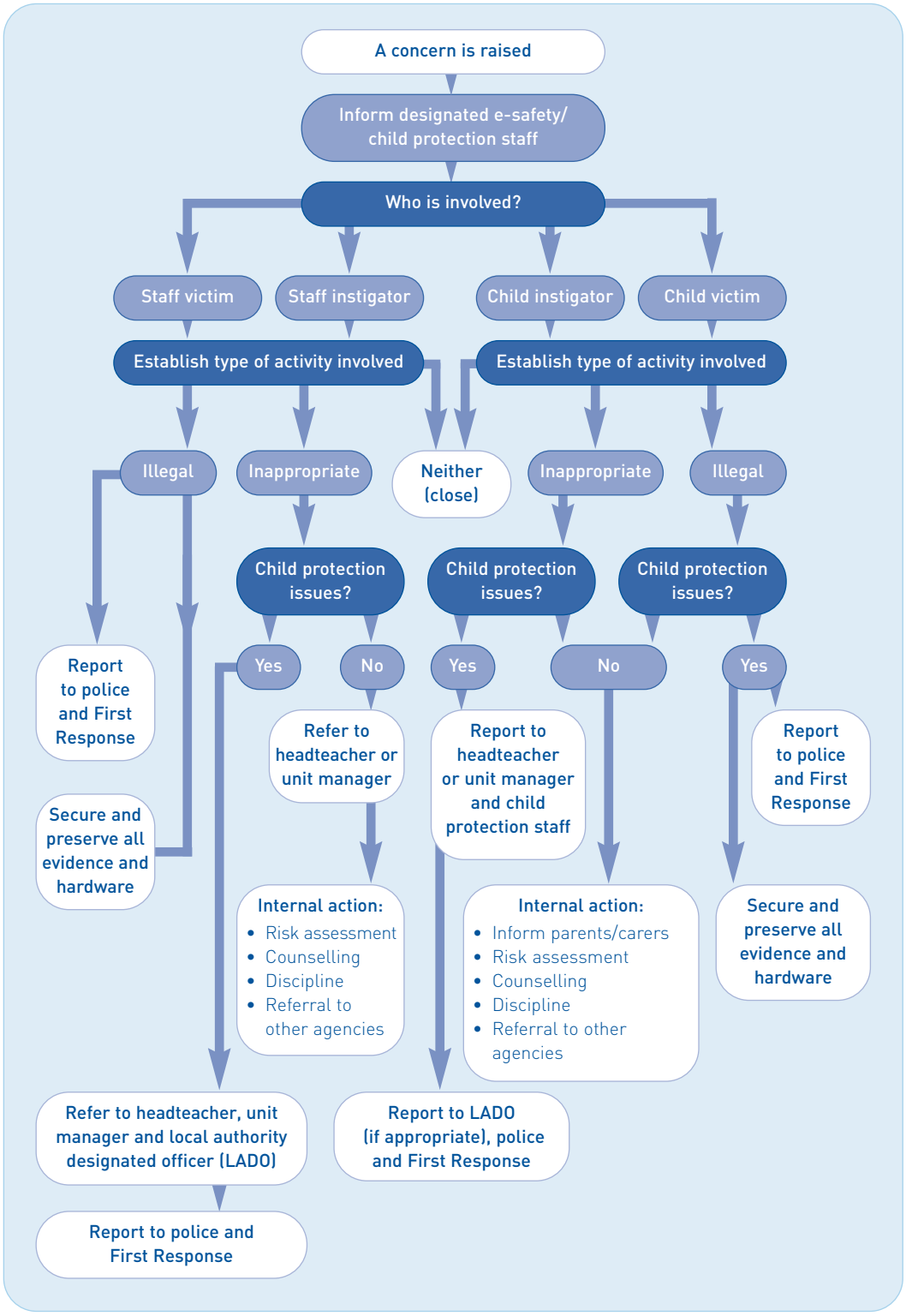


Chart 2

Staffordshire County Council E-safety incident flowchart



Notes on Staffordshire's First Response Service

It is not unusual for people to be uncertain about acting upon more unspecified concerns. Bearing in mind information-sharing legislation and guidance, and in particular the common-law duty of confidence, it is important that staff, volunteers and members of the public should feel able to share concerns in a responsible way. This may be achieved in a number of ways in Staffordshire, including the use of their 'First Response' telephone line.

First Response is the single point of access for all vulnerable children referrals which aren't currently open to a social worker. Information is taken from all agencies, parents/carers and children, and members of the public, including anonymous referrals.

First Response workers gather information, clarify this with the referrer, and offer advice and consultation. If the referral meets the criteria, it will be passed to the area offices for Children's Social Care for assessment or investigation.

Professionals and members of the public alike can consult the local authority's First Response Service, and they are informed at the outset that any information received which indicates that a child is suffering or is likely to suffer significant harm will be treated as a referral.

For further details please see **http://www.staffordshire.gov.uk/health/socialservices/childrenandfamilycare/childprotection**.

Chart 3

Northern Grid for Learning
Committing an illegal act – Did you know?

1. Receiving unsolicited emails that may contain potentially illegal material (either as an attachment or in a URL) is not an illegal offence
2. If you receive potentially illegal material you could easily commit an illegal act – **do not open the material or personally investigate**
3. Opening an attachment or URL that proves to hold illegal content **is an illegal act** and is classed as making of illegal material
4. Showing anyone else illegal material that you have received **is an illegal act**
5. Printing a copy of the offensive image to report it to someone else **is an illegal act** and is classed as making illegal material
6. Having printed a copy of the material if you give it to someone else **is an illegal act** and is classed as distributing illegal material
7. **Within 4 simple steps you could easily break the law 4 times. Each is a serious offence**
8. Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal, report it and log that you have received it
9. Always report potential illegal content to the Internet Watch Foundation at **http://ww.iwf.org.uk**. They are licensed to investigate, **You are not**

Never personally investigate. If you open illegal content accidentally, report it to the headteacher and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, but write it down and type it into the reporting screen. This prevents accidental opening.** Once the email has been logged and reported to the IWF, delete it from your inbox. If you are unsure, contact the IWF for advice on **01223 237700**. **The Internet Watch Foundation only deals with illegal content. Please see their website for information and advice. Please note this guidance only relates to illegal content, not inappropriate.**

Chart 4

Northern Grid for Learning
What to do with suspicious email

This diagram is provided for illustration purposes. Please amend it to reflect your own processes and protocols, and include details of your own internet service provider (ISP) as appropriate.

You receive an email that has potentially illegal material eg child abuse images, incitement to violence or race hate.	You receive an email that contains inappropriate content eg abusive or bullying content or adult sexual material This email is from someone you know within the school environment.	You receive an email that contains inappropriate content eg adult sexual material or bad language This email is not from someone you know but is from what seems to be a 'real' (ie not a spam) email address.	You receive an email that contains inappropriate content eg adult sexual material. This email is not from someone you know and appears to be a spam email.
Report this email to your headteacher and/or e-safety officer. A written log should be kept of the email and the fact that it was passed onto the IWF.	Report this email to your headteacher and/or e-safety officer. A written log should be kept of the email. An investigation within the school or LA should be undertaken.	Report this email to your headteacher and/or e-safety officer. A written log should be kept of the email and where it was sent for investigation.	Report this email to your headteacher and/or e-safety officer. A written log should be kept of the email and where it was sent for investigation.
Report this email to the IWF. Go to **http://www.iwf.org.uk**. Click on the report button and follow the instructions and their advice. **The IWF is the only organisation licensed to investigate illegal content.**	To escalate this investigation your school should contact the LA to authorise Northern Grid to investigate further. Sending such mails using the Northern Grid is not allowed under the AUP.	Contact your LA who will authorise Northern Grid to investigate. They will trace the sender's ISP and advise on further action (such as contacting the sender's school/organisation to raise a complaint under their AUP).	Report this to Easynet on **abuse@uk.easynet.net**.

In all cases secure the email in a folder and only delete when the investigation has been completed or you are advised to do so. In the case of potential illegal material, do not show the content of this email to anyone but report it to your headteacher and take the advise of the Internet Watch Foundation.

Do NOT always presume that the sender's email address is telling you the truth – spammers can and do fake others' email addresses.

Becta leading next generation learning

Responding to a RIPA notice

Part 1: Northern Grid for Learning
Procedure for investigations requiring disclosure of communications data

Part 2: Northern Grid for Learning
Protocol for disclosure of communications data

Part 3: Northern Grid for Learning
Proforma for disclosure of communications data

The following resource outlines the Northern Grid for Learning's approach to dealing with request for disclosures of communications information under the Regulation of Investigatory Powers Act 2000, otherwise known as RIPA.

Thanks to colleagues in the Northern Grid for Learning for sharing this material.

Part 1

Northern Grid for Learning
Procedure for investigations requiring disclosure of communications data

What to do if you need to or are requested to initiate an investigation

You are suspicious that a member of staff, parent, pupil or visitor may have been using the school network to gain access to potentially illegal material, eg child abuse images, or is suspected of inappropriate internet/email use.	Your LA contacts you regarding suspicions of data found about a member of staff and wants information from you to help in their investigations.	You are contacted by law enforcement or another government agency and asked for information to help their investigation.	Always ensure that you have the process and protocol in place before you start an investigation or provide information required for an external investigation. **Refer to the full guidance notes supplied.**
Ensure that your AUP clearly states that your network is monitored and that you have the right to investigate any suspicious behaviour. Contact you LA and ask for guidance.	Do not provide details or names until you are served with an internal RIPA from a senior member of staff in your LA. Always check that they are authorised to request this information.	Do not answer any questions and immediately insist they issue a RIPA notice. (They may try and persuade you by saying that this is delaying their investigations but do not be persuaded to divulge the information.)	Never provide information without the relevant legal request to do so. You may be placed under pressure to divulge without a formal request being issued – insist you are following correct procedures.
Ensure that proper procedures are followed and documented. If the behaviour is found to be illegal, you will be required to report it to the police. This is not an option, but a legal requirement.	Providing information without an official notice signed by the relevant member of staff is illegal under the Data Protection Act. **Use the guidance notes contained in this document.**	Providing information without an official notice signed by the relevant member of staff is illegal under the Data Protection Act. It can also hinder any ensuing court case. **Use the guidance notes contained in this document.**	Always keep copies of all notices and infomation provided. Ensure that this is kept secure. All of these investigations should be dealt with by a named senior member of staff.

It is crucial that you have an AUP that states clearly that your network is monitored and action will be taken against anyone misusing the network. These sanctions must be reflected in your behaviour policy.
Your school AUP should be signed by all members of staff, pupils, parents and visitors.
Do not be persuaded to divulge sensitive information without the correct procedure being followed.
Always check the validity of the request.

Part 2

Northern Grid for Learning Protocol for disclosure of communications data

Overview

In general, everyone is entitled to communicate with others confidentially and in privacy. For the common good there must be boundaries to this right; there must be means of detecting and countering wrongdoing. The extent to which police or other authorities or an employer or other provider of a communications system such as an intranet can legitimately monitor or intercept communications or be given information about them is controlled and regulated by law with a view to correctly balancing individuals' freedoms with child and general public safety and the detection and prevention of crime.

RIPA

The system set up by and the highly regulated powers given by the Regulation of Investigatory Powers Act 2000 (RIPA) enable confidential access to personal information, interception and covert surveillance to do with communications for law enforcement and other proper purposes where the access would otherwise be strictly forbidden (under RIPA itself, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the data protection or the human rights legislation and otherwise) including disclosure or surveillance of computer- and information-technology-based data and systems. The police, tax authorities, local authorities and other specified bodies with law enforcement or regulatory responsibilities are entitled to use these powers.

The key to this is a 'RIPA notice': a notice in standard form signed by a senior officer and sent by an investigator to someone that may hold or be able to obtain personal communications data needed in an investigation. A properly completed RIPA notice is a clear demonstration to its recipient that the information or access required by it is needed in complete confidence for a properly considered and justified purpose by an appropriate investigative authority. The RIPA notice is adequate justification for access to the information by the investigator per the notice. Unless there are compelling reasons not to, every correctly completed RIPA notice must be complied with in full within the time specified within it.

General duty of confidentiality

If you receive a communication from the police, your local authority, other law enforcement agency or another government agency (such as HM Revenue and Customs) asking for access to any personal information or data held within your school (for example information on members of staff, parents or families),

do not respond personally to this request unless you have clear authority to do so. Even if the contact stresses the importance and urgency of having this information, **do not** reveal any information unless you have authority.

If any information is given out without following a proper process, the individual officer and/or school may face, at best, serious complaints or, at worst, regulatory investigation and even legal proceedings.

A RIPA notice is sufficient authority for access to the communications-related access, information or data it requires.

RIPA procedure

Only specifically authorised law enforcement and government bodies may legally obtain access to confidential communications information from you by a formal written application using a RIPA notice.

If you receive a RIPA notice, you must respond to it within a given period of time. The RIPA notice will detail what information is required, why it is required to the extent that it is necessary to confirm this, who the investigating officer is and who is the authorising officer.

Following a considered process when dealing with a RIPA notice will help to prevent any future problems and will answer concerns about whether access to the relevant confidential information has been lawful.

It is very important to ensure that the RIPA notice you receive has been completed correctly and has been signed. **There is a special procedure for most exceptional speed where lives are at immediate risk or there are other matters of the gravest kind. You will be advised about this by the investigating officer in the unlikely event of this special procedure being clearly necessary.** Under these circumstances it is imperative that you take advice from your LA legal department before any disclosure is made.

It is also important to ascertain that the person sending the notice, whether in person, by letter or by fax is a *bona fide* officer. This can be done by contacting the local or central government office or police force that originated the RIPA notice. Keep a record of which office you contacted, the date and time of your contact and from whom you gained confirmation.

Once you are satisfied that the RIPA notice received is correct and you have validated the requesting officer, you must then provide the information requested. It is important that you provide **only** the information or access requested and no more. **Do not** elaborate or add extra information because you think it may be useful. Only the information or access detailed by the requesting officer is protected by the RIPA notice.

If something further is required, the requesting officer will serve another RIPA notice detailing the new request.

Photocopy the RIPA notice and the response you make to it. Keep a file of this and the record of the validation process followed. This data will need to be stored securely as it may be called upon as evidence of your correct conduct.

It is important that all relevant documentation and information should be held confidentially. In particular, it should be noted that 'tipping off' the apparent target of any RIPA notice or indeed anyone else could be a criminal matter.

Local authority request for information

Your school's local authority has statutory powers under the education acts, within employment and tax law and otherwise to require, hold and use personal data relating to the school's pupils, their parents and carers and staff. The procedures and systems for gathering and transmitting this information are routine and are well structured with a view to ensuring that the relevant laws are complied with.

If, outside the routine pupil and staff data regimes, your local authority requests access to sensitive data regarding a member of staff, pupil or family as part of an investigation, you should insist that they put this request in writing as would any other investigating public body and only provide the information if you have a clear authority to do so. As appropriate in respect of communications matters, you should act only on a RIPA notice. Only nominated senior members of staff have the authorisation or investigation powers that entitle them to request this kind of information using a RIPA notice.

As you would more generally, you should follow the RIPA procedure for validation and keep a record of the request, validation and information supplied.

Some local authority investigators (especially those that have no day-to-day role in education or other children's services) may not immediately understand that a school governing body has separate legal standing and status and is for these purposes not simply and indivisibly part and parcel of their local authority. A simple explanation of this may prove helpful in making quick progress in these matters.

All records should be kept securely and by a senior member of staff.

Advice

This note is intended to be no more than an overview in outline of and pointers about one aspect of what is a complex, potentially contentious and quickly developing area of law and best practice. Your local authority should be able to provide its definitive written policies and someone from whom you can seek independent and confidential legal advice on any point of difficulty. This will usually be someone from the authority's in-house legal team.

Status of RIPA notice information

Information gathered by an investigator using a RIPA notice is most usually intelligence rather than evidence to be used in court. The information will typically be used to progress, develop or conclude enquiries, quite possibly without any further reference to you or indeed any individual named in the RIPA notice. It is entirely possible that any individual mentioned in a notice is not suspected of any crime or, if suspected, is in fact demonstrably innocent of any wrongdoing on further enquiry.

References

- RIPA Home Office website
  [**http://security.homeoffice.gov.uk/ripa/about-ripa**]
- Office of Surveillance Commissioners
  [**http://www.surveillancecommissioners.gov.uk/advice_ripa.html**]
  Provides useful guidance for local authorities.

Part 3

Northern Grid for Learning Proforma for disclosure of communications data

Name of requesting body:	
Name of requesting officer:	
Name of authorising officer:	
Contact telephone number:	
Email address:	
Personal identifying registration: (eg police number, rank or position)	
Verify validity of requesting officer:	Alternative contact details used: Authenticate personnel: Validate request for information:
Details of request:	
Reason given for request:	
Signature of named authorised personnel providing data:	
Additional comments:	

Date of initial request			**Date notice received**			**Copy of notice attached? TICK in box**			**Date notice returned**		
Notice returned by recorded delivery	**Y**	**N**	**Completed by (initial of member of staff)**			**Chair of governors informed**	**Y**	**N**	**Copies sent to Chair**	**Y**	**N**
Notice returned by fax	**Y**	**N**									

Becta leading next generation learning

Example LSCB training activities

Recommendations for using these materials

Part 1: E-safety dilemma cards

Part 2: Who should be involved in e-safety incidents?

Part 3: E-safety dilemmas – What happened next?

Part 4: Safeguarding and e-safety flowchart
Practical questions and reflective points

Part 5: Safeguarding Sam mapping resource

Thanks to colleagues in the London Borough of Havering and the Royal Borough of Kensington and Chelsea for sharing these materials, and thanks to those who attended the e-safety working days for their input.

D

Recommendations for using these materials

1. Use the **e-safety dilemma card** activity (**Part 1**) to improve personal understanding of the safeguarding and e-safety issues that children and young people may be involved in. In small groups, discuss a selection of the cards, identifying both the possible risks and consequences and the possible actions. In some cases, you may need to acknowledge that the adult perception of the risk may be an overreaction.

   Categorise the risks into three categories:

   There is little or no danger to the young person – the activity is one they may continue with.

   Encourage safe behaviour – the young person should be supported in their e-safety activity. They should stop the activity or take no further action.

   There are significant e-safety risks, and the incident must be escalated – this may involve reporting the activity to the service provider (for example, phone company or internet service provider), reporting abuse (for example, to CEOP or the police) and/or involving local authority support services.

2. Using a selection of the dilemma cards that the groups assessed as posing a significant risk, consider the generic groups of people within your local authority (and beyond) that may need to be involved in an e-safety issue. Use the **Who should be involved...** grid (**Part 2**) to record your thoughts.

3. Use the more detailed **What happened next?** scenarios (**Part 3**) to develop further understanding of a selection of the scenarios considered in exercise 1. Consider developing more scenarios as part of the training activity.

4. Use the **practical questions and reflective points sheet** (**Part 4**) to assess your own personal and professional readiness should an e-safety issue arise. You may use this question sheet for gap analysis, looking at the process as well as at training and development needs.

5. Use the **Safeguarding Sam** resource (**Part 5**) to look at specific services within and supporting your authority. Use this generic map to record details of points or contacts. Consider which other services are specific to your local situation.

6. Use the **longer case study** materials at **Annex F** to consider your readiness as an LSCB for a significant issue. Look at the mistakes made and use this to inform your current and future practice.

Part 1

E-safety dilemma cards

Dilemma cards to be cut out or photocopied for use in small groups to identify the risks and consequences of e-safety issues.

Felix is 12. He is using the internet in his bedroom when a message pops up on his screen: 'Hey I'm Justin and I'm 10 years old. I'm looking for a friend in England. Click here to send me an email.'

Millie is in an internet café, trying to find pictures for her project about big cats. By accident, she finds some pictures and photographs that make her feel uncomfortable and embarrassed.

At home Osian is using Instant Messenger (like MSN). One of his online 'friends' asks him for his address and telephone number.

Kiereen is in Year 7. She has received a text message on her mobile. It says 'We h8 yuhh. We r goin 2 get yuhh l8r.'

Lois's friend offers to share their Instant Messenger (like MSN) contacts. Lois is very pleased because she now has 150 'friends'.

Lee is 10. He gets a text message on his mobile saying: 'Cool ring tones. Just text YES to download.'

James is seven years old. He's in a chat room – a pizza parlour in a 'virtual' world. Someone is 'talking' to him and asks if he wants to chat 'outside' and can they swap email addresses?

Surika is thinking about signing up to a new 'cool' site where she can post pictures and talk to others. There's a page where she can put her profile. It asks her for all her personal information.

Jago's friend has set up a site on MySpace, even though they are not old enough to join the site. His friend hasn't thought about using the privacy settings. Jago is looking at it and sees that they have put some photos of him on their site.

David has been 'talking' to a 'friend' on MSN and they ask him to go on webcam. After a while, they ask him to do things that he doesn't feel comfortable with.

Shona's friend has been on a diet for a long time and is now really thin. The friend shows Shona some websites with very thin models and keeps going on about how she wants to 'look like them'. Shona's friend is very unhappy about how she looks and doesn't seem to see how she is making herself ill.

Ahmed has received a surprise email saying: 'Your details have been safely received. Please confirm by clicking on the link below. You could win a digital camera.'

Jack has been talking to an online 'friend' for some time. The 'friend' seems really nice and they have loads in common. They've sent Jack a photo of themselves. It's the holiday and they ask Jack to meet in the park.

In an ICT lesson in school a big star appears on Anika's screen. It flashes, and these words appear: 'You have won £100! Click here now to get your prize!'

Isobel's friend is feeling down. The friend has been spending lots of time online talking to others who feel the same. Isobel is worried that her friend is taking advice from those people.

Karl's friend shows him a website their older sister uses to buy things online. She is still signed in because she's bidding for a mobile phone. Karl finds an item which he would like. His friend says, "Let's make some bids!"

For a while Sophie has been chatting online in secret with someone older than her. At first he seemed really nice and appeared to understand her better than her family. She knew it was silly, but she found it easy to tell him lots of personal things, and she was pleased to have an 'older boyfriend' online. But now he is sending her very personal and 'explicit' messages which make her feel uncomfortable and uneasy about the 'relationship'.

Edith overhears some classmates talking about a personal website. She visits it and find it's horrible about her, and there is even a 'vote' to see who hates her.

Sharima is proud of her blog: she writes it for three friends and tells them everything. Sharima is 14. She's also blogging her emerging sexual experiences.

On the school bus Liam had his trousers pulled down and some other pupils videoed the incident on their phones.

A teacher finds a USB memory stick in the playground. The files on it are photographs which include some of teenage girls partially dressed. The owner of the USB stick is not known and the teacher does not recognise the girls in the photos.

Paige was very upset when she split up with her boyfriend. She really wanted him back. She used her mobile phone to take a topless photo of herself to show him what he was missing, wrote her phone number on her stomach in lipstick and added 'call me'. Chris doesn't want Paige back: she's 13 and too young for him. He posts Paige's photo on his website to humiliate her.

Mr Webster's classroom internet computer is taken away for repair. The engineer finds adult pornography on the computer. The computer, which was donated, did not have the virus and firewall software added when it came into school.

Mrs Morisson takes Year 9 for history in the ICT suite. One boy is found printing out hardcore adult pornographic images on the classroom colour printer.

A teacher's school laptop is sent for repair. An abusive image of a child is found in the folder that holds temporary internet files.

A social worker visits a sex offender at home. The offender lives with his family, including his preteen daughter. She has her own computer with a webcam.

Jess and Dan are visiting secondary school open evenings with their daughter. In one school they pick up a piece of paper which has IDs and passwords for some of the pupils and staff.

Mubo, in Year 5, has her own Piczo website. A teacher at another school stumbles across it when looking at sites their pupils have shown them. Mubo has put up photos (labelled), full home details, her route to school, her social activities each week – and more.

A 14-year-old boy has taken his own life. There is an allegation of bullying and a website emerges that has hate comments about the boy and also message board posts which say they are glad he is dead.

Elliot is 12 and has a new mobile phone. It has an instant link to his website to upload photos. He has already posted photos of his pet corn snake and his brother's motorbike. On the way to school a Year 12 pupil grabs his phone.

Rashid is 10 years old. He spends long hours playing an online game called Runescape. His best friend in the game is Obi, who is also 10. Rashid gets very grumpy when asked to leave his computer. He has stopped watching TV and he locks his door when he is game playing.

Russell is 15. His blog is used by young people in the local area to find out where drugs are on offer. No one knows who Russell is. His site is changed every day.

Sunshine Primary School has a new ICT installation across the school. The school used a local company and has a technician in the school working on the network one afternoon a week. The technician comes from a pool.

Joe is in Year 1. He has access to the internet in his bedroom and plays in a virtual world. He talks about Tom, who is also 7, and Joe is really 'happy to have a new friend'.

Reece is really worried about his mum. She has signed up to an online dating agency and he knows she is going off to meet strangers.

During a discussion in a Year 1 class, 55% of the children say they have had online experiences which are embarrassing or uncomfortable.

Jetinda lives in a town, but he is quite isolated, has very few friends and spends long hours online. He has a new mobile phone with a moblogging facility. He has collected mobile phone numbers from online 'friends' and sends them moblogs, sometimes several times a day.

Georgia has a new bank account. She has a Visa electron card and can use cash points. She receives an email from her bank asking her to go to a website to confirm her personal details and pin number.

Amanda doesn't want her son to use the internet. The computer at home has no connectivity. She buys him a new Sony PSP so that he can play games in his bedroom.

A class of 8-year-olds are in the ICT suite. The teacher gives them a research topic: 'Thailand'. Robert calls the teacher over to tell her that the search results include a link 'adult sex'. The teacher says "Don't click the link," and then moves away to talk to another group of children elsewhere in the classroom.

Part 2

Who should be involved in e-safety incidents?

E-safety incident				
Who should be involved? **In what order would you notify those involved? (Number with 1, 2, 3)**	Young person			
	Family			
	School/education provider			
	Governors			
	LSCB (named e-safety contact)			
	Social care			
	ISP (internet service provider)			
	Regional grid			
	Health authority			
	Police			
	IWF (Internet Watch Foundation)			
	CEOP (Child Exploitation and Online Protection Centre)			
Rationale				

Part 3

E-safety dilemmas – What happened next?

Felix is 12. He is using the internet in his bedroom when a message pops up on his screen: 'Hey I'm Justin and I'm 10 years old. I'm looking for a friend in England. Click here to send me an email.'

Felix knows that his email address is private. He doesn't share it with strangers. He ignores the message on screen and clicks on the x in the top-right corner to close it down.

Millie is in an internet café, trying to find pictures for her project about big cats. By accident, she finds some pictures and photographs that make her feel uncomfortable and embarrassed.

Millie was uncomfortable because she didn't like the images she saw and she was worried someone had seen her in the café and that she would be blamed. She went home and told her mum, who reassured her that it wasn't Millie's fault and talked to her about the image content. Millie felt reassured. She said she felt she could tell her mum about internet problems.

At home Osian is using Instant Messenger (like MSN). One of his online 'friends' asks him for his address and telephone number.

Osian thinks about giving out his details, but decides to talk to a friend in school that shared their contacts with him. They tell Osian that the 'friend' is their cousin and that he will be at their bowling party on Saturday. Osian is already invited. His dad takes him to the bowling party and they both meet Osian's new friend.

Kiereen is in Year 7. She has received a text message on her mobile. It says 'We h8 yuhh. We r goin 2 get yuhh l8r.'

Kiereen is unhappy about the message. Children in school have been saying unkind things. She talks to her form tutor and shows her the message. Her school takes the bullying very seriously and Kiereen does not feel alone any more.

Lois's friend offers to share their Instant Messenger (like MSN) contacts. Lois is very pleased because she now has 150 'friends'.

Lois's 'friends' have been collected by sharing address books. She only knows about a third of the people in her contact list. She has used the features in MSN to sort her 'friends' into groups – school, home friends, family, holiday mates. She also has a group for 'friends of friends' ie internet strangers. She does not give out any personal details to these people. She is happy to chat online with friends of friends, but nothing more. She does not use her webcam when she talks to this group.

Lee is 10. He gets a text message on his mobile saying: 'Cool ring tones. Just text YES to download.'

Lee replies to the text and says YES. He gets sent two ring tones that day and two more the day after. He notices he has no credit left and that he has had four charges to his phone that add up to over £10. His mum helps him cancel the subscription. They are both glad Lee is on 'pay as you go', because it limited the amount the ring tone company could take from Lee's mobile phone account. Lee told all his friends what had happened, as he did not want them to be duped as well.

James is seven years old. He's in a chat room – a pizza parlour in a 'virtual' world. Someone is 'talking' to him and asks if he wants to chat 'outside' and can they swap email addresses?

James is sitting with his mum; they are using the internet together. James' mum explains he should never give out his private information to anyone, and, if he is not sure, he should talk to a grown up at home or at school.

Surika is thinking about signing up to a new 'cool' site where she can post pictures and talk to others. There's a page where she can put her profile. It asks her for all her personal information.

Surika decided she didn't want to put in her own information, but she did fill the form in. She invented a new persona for herself and used that instead.

Jago's friend has set up a site on MySpace, even though they are not old enough to join the site. His friend hasn't thought about using the privacy settings. Jago is looking at it and sees that they have put some photos of him on their site.

Jago emailed his friend to say he was worried that his site was not private. He tells his friend to look at his own website to get some ideas about how to keep a site safe. He takes his friend's site off his friends list, but adds it back in once his friend has worked on his site to make it safe.

Shona's friend has been on a diet for a long time and is now really thin. The friend shows Shona some websites with very thin models and keeps going on about how she wants to 'look like them'. Shona's friend is very unhappy about how she looks and doesn't seem to see how she is making herself ill.

The girl's friends talk to each other; they are all worried and want to support her. They are not sure what to do, so they decide to tell someone whom their friend would trust and whose opinion she would value. The friends all attend an evening drama group and they talk to the drama group leader.

Ahmed has received a surprise email saying: 'Your details have been safely received. Please confirm by clicking on the link below. You could win a digital camera.'

Ahmed realises that this is a scam. He knows that the email is automatically sent to thousands of email addresses and that replying will send information about an active email address which could result in loads more spam email. He ignores the email, deletes it and tells his friends and his teachers about it in case they receive it too and don't know what to do.

Jack has been talking to an online 'friend' for some time. The 'friend' seems really nice and they have loads in common. They've sent Jack a photo of themselves. It's the holiday and they ask Jack to meet in the park.

Jack likes his friend and would like to meet him. He tells him he'll see him on Saturday and he'll be bringing his dad. His friend says 'OK' and that his dad will be there too. They have a good kick about in the park and the dads find a coffee stall!

In an ICT lesson in school a big star appears on Anika's screen. It flashes, and these words appear: 'You have won £100! Click here now to get your prize!'

Anika knows it is an advertising pop up. She closes the window and gets on with her work.

Isobel's friend is feeling down. The friend has been spending lots of time online talking to others who feel the same. Isobel is worried that her friend is taking advice from those people.

Isobel finds out the details of ChildLine as she thinks her friend needs someone to talk to. She types all the details into Word and prints out a note for her friend. She puts on a couple of photos of them together having fun.

Karl's friend shows him a website their older sister uses to buy things online. She is still signed in because she's bidding for a mobile phone. Karl finds an item which he would like. His friend says, "Let's make some bids!"

Karl isn't sure what to do, but he realises that even if he wins the item he won't be able to pay for it. He has used eBay at home. He uses an option in eBay to send himself an email giving the details of the item so he can look at it later.

For a while Sophie has been chatting online in secret with someone older than her. At first he seemed really nice and appeared to understand her better than her family. She knew it was silly, but she found it easy to tell him lots of personal things, and she was pleased to have an 'older boyfriend' online. But now he is sending her very personal and 'explicit' messages which make her feel uncomfortable and uneasy about the 'relationship'.

Sophie doesn't go online for a few days. She doesn't talk to anyone: she's too embarrassed to talk about this to anyone face to face. She remembers a lesson at school where she learnt about a red button, so she looks in MSN and finds it. It says 'report abuse'. She types all the details into the form. She feels better for having told someone. She doesn't talk to her 'boyfriend' again.

Edith overhears some classmates talking about a personal website. She visits it and find it's horrible about her, and there is even a 'vote' to see who hates her.

Edith talks to her parents. They contact the school and talk to the year group head. Her parents also report the page to the social networking site: the group of youngsters are underage for the site. The website is taken down.

Sharima is proud of her blog: she writes it for three friends and tells them everything. Sharima is 14. She's also blogging her emerging sexual experiences.

Sharima doesn't realise her blog is public. She hasn't completed the profile information on the site, but her friends are worried that she will reveal personal information. They try to talk to Sharima, but she tells them not to worry. Some of her blog is exaggeration, but she is enjoying the reputation she has: it makes her feel important. This dilemma is not resolved. Sharima's friends continue to worry about her. They told a responsible adult, but would not reveal Sharima's blog web address or her name.

On the school bus Liam had his trousers pulled down and some other pupils videoed the incident on their phones.

The bus driver, who knew about 'happy slapping' videos, witnessed the event, stopped the bus and called the school. The videos were not posted on a website. The pupils were disciplined, and Liam was supported and other bullying incidents investigated.

A teacher finds a USB memory stick in the playground. The files on it are photographs which include some of teenage girls partially dressed. The owner of the USB stick is not known and the teacher does not recognise the girls in the photos.

The teacher talked to the community police officer for the school, who recommended finding the owner of the memory stick rather than trying to identify the girl. Other files on the USB stick were used to identify the owner of the memory stick. The photographs were of a teenage girl in another school. They had been taken by a boyfriend and were circulating without the girl's permission. The extent of circulation was established. It was not possible to be certain these photographs had not ended up on the internet. The girl and her parents were talked to by pastoral staff at her school.

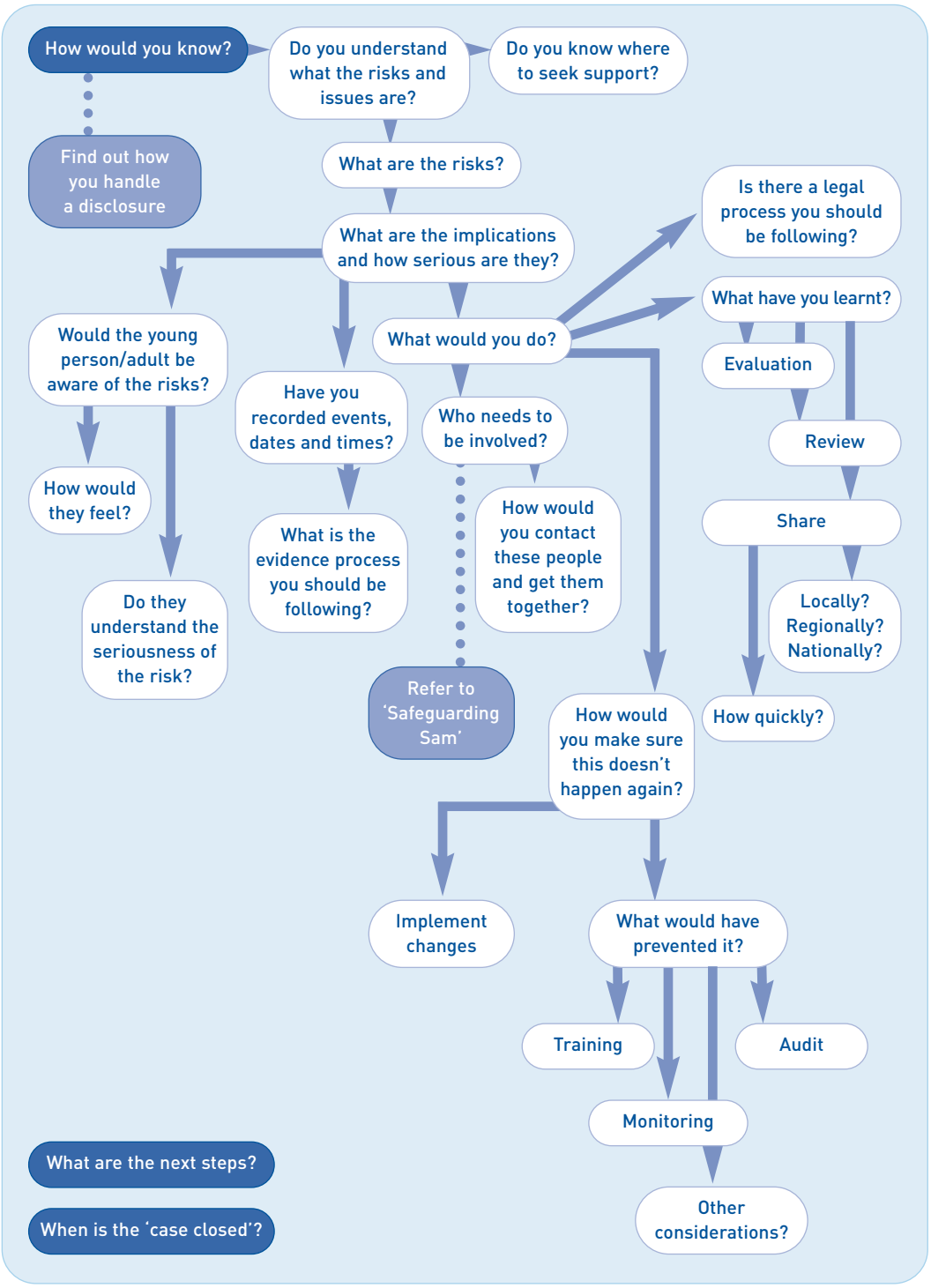
Mr Webster's classroom internet computer is taken away for repair. The engineer finds adult pornography on the computer. The computer, which was donated, did not have the virus and firewall software added when it came into school.

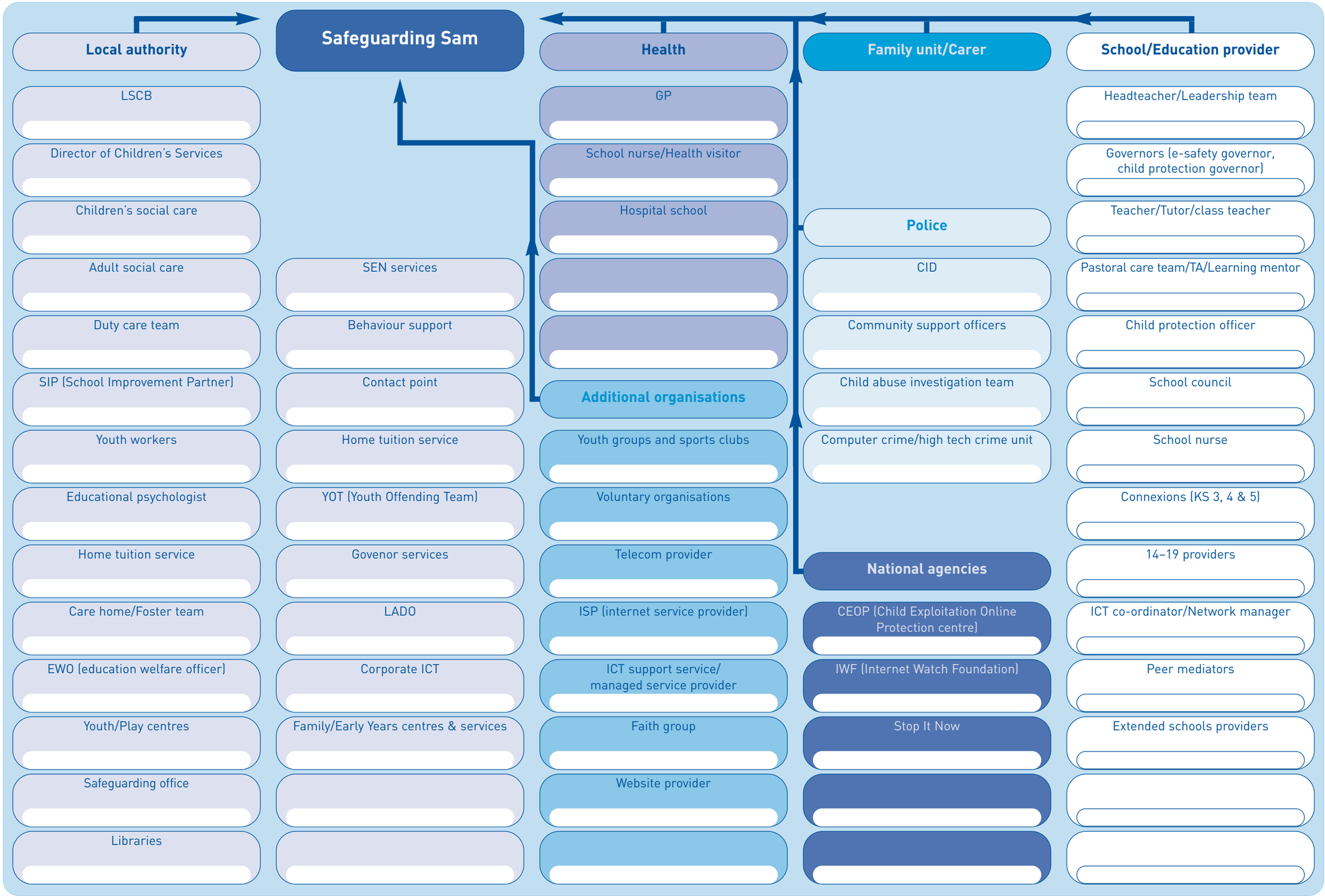
Because the images were of adult pornography, the police were not called. The files were investigated and the date and time showed that they were on the PC when it was donated. The school did not go back to the parent that donated the PC (their child had by then left the school). The school revised its policy about donated equipment and the measures that should be taken to ensure that the hard disks were wiped (both when receiving and disposing of equipment) and the necessary software installed. Once the school realised that it would have to pay hardware disposal charges (following the EC Directive on Waste Electrical and Electronic Equipment (WEEE)[29]), the policy was further revised to decline donated equipment. The school recognised that the hidden costs of donated equipment were high and the equipment offered was out of date.

[29] See Directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003 on waste electrical and electronic equipment (WEEE) [**http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_037/l_03720030213en00240038.pdf**].

Part 4

Safeguarding and e-safety flowchart practical questions and reflective points





Where possible list contacts for 24/7/365

Becta leading next generation learning

CEOP Practice guidance for teachers

The Child Exploitation and Online Protection (CEOP) Centre has contributed the following practice guidance for teachers.

Safeguarding and promoting the welfare of children and young people through the Thinkuknow education programme

Preface

This practice guide has been issued to assist teaching staff within schools where the Thinkuknow education programme is being delivered to pupils.

The document recognises that concerns about a child's welfare may become apparent as a result of a pupil's being empowered to report a child protection concern either during or following the Thinkuknow education presentation. It recognises that concerns reported to teaching staff about a child's welfare may vary greatly in terms of the nature and seriousness of those concerns, how those concerns are reported and over what duration they have arisen.

This document focuses on:

- What teaching staff should do if they have child protection concerns in order to safeguard and promote the welfare of children
- What will happen once teaching staff have informed statutory agencies about those concerns
- What further contribution teaching staff may be asked or expected to make to the process of assessment, planning, and working with children.

This guidance has been produced by the Child Exploitation and Online Protection (CEOP) Centre. It summarises the key processes but does not replace *Working together to safeguard children* (2006) or the *Framework for the assessment of children in need and their families* (2000).

Safeguarding and promoting the welfare of children within schools... What does this mean?

Safeguarding and promoting the welfare of children is defined in statutory guidance under the Children Acts 1989 and 2004 as:

- Protecting children from maltreatment
- Preventing impairment of children's health or development
- Ensuring that children are growing up in circumstances consistent with the provision of safe and effective care
- Undertaking that role to enable those children to have optimum life chances and to enter adulthood successfully.

The Children Act 1989 places a duty on schools to safeguard and promote the welfare of their pupils by:

- Creating and maintaining a safe learning environment
- Identifying where there are child welfare concerns and taking action to address them, in partnership with other organisations where appropriate.

Schools also contribute through the curriculum by developing children's understanding, awareness and resilience. Teaching staff also have a crucial role to play in helping to identify child welfare concerns and indicators of abuse and neglect at an early stage, and then to refer those concerns to the appropriate agencies.

The concept of 'significant harm'

Some children in schools may be classed as 'children in need' because they are suffering or likely to suffer 'significant harm'. Significant harm is a concept that refers to the threshold that justifies compulsory intervention in family life in the best interest of children. It gives local authorities a duty to make enquiries to decide whether they should take action to safeguard and promote the welfare of a child who is suffering or likely to suffer significant harm.

A local authority children's social care department is under a duty to make enquiries where 'it has reasonable cause to suspect that a child is suffering or likely to suffer significant harm'. This involves making necessary enquiries to assess what is happening to a child, concentrating on the harm that has occurred or is likely to occur as a result of child maltreatment in order to inform future plans to safeguard and protect the child.

Decisions about significant harm are highly complex and should always be informed by careful assessment of the child's circumstances and discussion between educational staff with the statutory agencies. **It is not the responsibility of teaching staff alone to form a view as to whether a child has suffered or is likely to suffer significant harm.**

Abuse and neglect of children

Abuse and neglect of children are forms of maltreatment. A person may abuse or neglect a child by inflicting harm or failing to act to prevent harm. The Children Act 1989 provides clear definitions of the four main categories of abuse: physical abuse, emotional abuse, sexual abuse and neglect.

Child abuse and information communication technology (ICT)

The range of child abuse definitions and concepts (as defined within the Children Act 1989) are now being seen in ICT environments. As new and emerging technologies develop, so will the motivation of those intent on abusing children to use technology to facilitate their abuse of children. In particular, the internet has become a particular tool in the distribution of abusive images of children. Internet chat rooms, peer-to-peer discussion forums and the new phenomenon of 'social networking' are now being used as a means of contacting children with a view to grooming them online for inappropriate or abusive relationships either online or offline. This can involve inciting children to make and transmit indecent images of themselves or perform sexual acts in front of a webcam. There is also a growing concern about the number of children meeting up with people in the real world whom they first met online.

Thinkuknow education programme

The Thinkuknow education programme being delivered in your school is a resource developed by CEOP to help children learn about the risks they may encounter while using the internet or other interactive technology. It has a number of themes to focus on three key messages:

- How to have fun online
- How to stay in control online
- How to report a problem.

Children and young people will be taught how to:

- Recognise and manage potential risks associated with their online activities
- Behave responsibly online
- Judge what kind on online relationships are acceptable and unacceptable
- Recognise when pressures from others in the online environment may threaten their personal safety and wellbeing and how to develop effective ways of resisting pressure
- Stay in control and report a problem.

Child welfare concerns reported to teaching staff either during or following the Thinkuknow programme

Thinkuknow has been designed to be emotionally engaging and impactful in terms of getting the above key messages over to children. It is interactive and uses a number of powerful short films to educate children about the risks they may encounter when using the internet. Importantly, it seeks to empower children to know how to report a problem, including abuse.

Teachers should be mindful that there may be occasions when, as a result of a child or young person participating in Thinkuknow, he/she may feel empowered to report an abusive situation to a teacher or a trusted individual within your school.

Teachers also need to be mindful that there may be children participating in the Thinkuknow programme who have previously been the subjects of inter-agency child protection procedures. In these situations, it is important that teaching staff know how to respond appropriately. Consequently, where possible your school's 'designated child protection officer' should be present during the Thinkuknow presentation and prepared to respond to any child protection concerns that may arise.

The designated child protection officer should be familiar with the locally agreed child protection procedures and the process for referring on child welfare concerns to the appropriate safeguarding agencies.

It is particularly important that on the day Thinkuknow is being presented in schools, teaching staff know exactly whom to contact in children's social care and the police, should a staff member become concerned about a child's welfare.

What to do if a child reports abuse to a teacher either during or following the Thinkuknow programme

The following are the basic steps that teaching staff are advised to follow in the event that a child wishes to confide in a teacher that he or she is likely to be at risk.

- Create a safe environment for the child by taking the child to a private area within the school.
- Stay calm and listen carefully to what the child has to say, taking what the child says seriously. If the child starts to confide in you about a potentially abusive situation, acknowledge that this may be difficult for the child.
- If the child does report a child protection concern, reassure the child that he/she is not to blame, but do not promise confidentiality.
- Be honest with the child and do not make promises you cannot keep. In particular, explain that you will have to tell other people in order to help them and explain that you will not be able to keep it a secret.
- Try to be clear about what the child is saying to you and keep questions to a minimum, avoiding closed questions. Allow the child to use his/her own words and avoid the child having to repeat what they are telling you.
- Remember that an allegation of child abuse reported either during or following the Thinkuknow programme or at any other time may lead to a criminal conviction. Consequently, avoid doing anything that may jeopardise a police investigation such as asking leading questions. Once the initial concerns have been reported to you, discuss your concerns with the designated child protection officer in your school or the headteacher.

- The designated child protection officer at your school should immediately refer the matter to the LA children's social care department in line with the locally agreed inter-agency child protection procedures. While teachers should seek, in general, to discuss any concerns with the child's family and, where possible, seek their agreement to making the referral to the LA children's social care department, this should only be done where such discussion and agreement-seeking will not place a child at increased risk of significant harm. Sharing of information in cases of concern about children's welfare enables professionals to consider jointly how to proceed in the best interest of the child and to safeguard children more generally.
- When making the referral to children's social care, you can expect the recipient of the referral to clarify with you the nature of the concerns, how they have arisen, what action you should take next and particularly what the child and the parents will be told, by whom and when.
- You will be required to make a written record of what the child reported to you and your responses. This must be done as soon as practicably possible and within 12 hours.
- If you are referring an alleged incident of contemporary abuse to the children's social care, it is likely that the matter will immediately be referred on to the police and an initial strategy discussion would ensue. The strategy meeting will decide whether to initiate enquiries under section 47 of the Children Act 1989 and therefore to commence a core assessment. It will also consider the necessity for emergency protective action to protect the child.
- Dealing with child protection matters can be stressful and emotionally demanding. Teaching staff are encouraged to seek support from line managers and occupational health support staff.

Becta leading next generation learning

Safeguarding incident case studies

Case study 1: Child abuse images – a potential scenario

Case study 2: Revelation of abuse – a potential scenario

Case study 3: Cyberbullying – a potential scenario

These potential e-safety scenarios are intended to act as discussion prompts to get LSCBs thinking about how they might tackle such safeguarding situations within their own local context.

Thanks to colleagues in the London Borough of Brent for sharing these case study scenarios.

F

Case study 1

Child abuse images – a potential scenario

The referral

A social worker receives a call from an independent fostering agency. The agency in turn has been contacted by one of its foster carers, Mrs Clay, who has a looked-after child, Peter Raymond, placed with her.

Mrs Clay has told the agency that her adult son, Marcus, has found images and videos of child abuse on a computer in the home. The computer belongs to Peter. It is not connected to the internet but Mrs Clay stated that Peter often took his computer with him when he went to stay elsewhere. It is not a laptop. She said that he spends a great deal of time on it.

Mrs Clay informed the fostering agency that Peter was not aware of the files being found. She also stated that Peter was spending a lot of time away from the home. She did not know where he was staying when he was away, but thought he might be staying at his mother's.

A week has elapsed between the agency receiving this call and any contact being made with social care.

The background

Peter Raymond is almost 18 and has been looked after in a variety of settings since he was 10.

He initially came into care following allegations of sexual abuse made against his father, Mr Raymond. These allegations were made by a paperboy at a newsagent's run by Mr Raymond.

There had been an allegation of abuse made against Mr Raymond in the past, in that case by a neighbour about her son. This was felt to be malicious. Further to this, however, there had been concerns in the past about Peter. The school had reported that he had been exhibiting sexualised behaviour. Social care had conducted an initial assessment, but it was felt that the concerns were not substantiated.

Following investigations into the paperboy's allegation, social services and the police believed that Mr Raymond had sexually abused the paperboy and had also sexually abused Peter. The Crown Prosecution Service, however, would not take the case to court owing to a lack of evidence.

Peter's mother stuck by her partner, denied the substance of the allegations and remained in close contact with him. Though he claimed to have moved out, it was believed that he was living in the family home. Peter spent a period on the child protection register but it was finally felt that Mrs Raymond was unable to protect her son and he was placed in care on a full care order.

Though six months later she separated from Mr Raymond, Peter's mother swiftly found a new partner and had a daughter, Donna. Donna is five at the time of this referral and was subject to a Section 47 investigation last year following concerns from Donna's nursery about neglect and sexualised behaviour. Donna was placed and remains on the child protection register for neglect.

Though Peter is not living in the home, it is believed that he often stays with his mother, sometimes for long periods. It is also believed that he has been visiting his father at his father's address. The foster carer is often unsure where he is.

Despite these concerns, Peter's current placement had been considered stable and he has been there for four years. Peter has not been engaging fully in education, although he has recently completed an ICT course. He has long held an interest in ICT and this is the second course that he has completed. He specifically asked for some of his savings to be released to enable him to buy a computer.

Peter will be 18 in two months. The plan is for him to return to his mother while semi-independent accommodation is sought.

What happened next?

Peter's social worker convened a strategy meeting attended by the Referral and Assessment Duty Manager, an officer from the Police Child Abuse Investigation Team, a Leaving Care Team social worker and the independent fostering agency (IFA) link worker.

- Discussion focused on the nature of the images themselves and the whereabouts of Peter and the computer.
- It emerged that the IFA link worker had already visited the placement to support the foster carer and spoken to Peter. Though they had not directly mentioned the images, it was felt that this may have made him aware that they had been found.
- It was heard from the IFA that Peter was not staying at the foster carer's home and had taken his computer with him.
- There was a lack of clarity about which section of the police should be dealing with this. The Child Abuse Investigation Team felt it was not their remit, but were unsure as to whether the police's Sapphire sexual abuse team or CID should be tackling the case.
- The social care duty manager wanted social workers to view the images as they were unsure of the nature of the images.
- It was agreed that a joint police/social care interview would take place with Peter about the images.
- The police were to pursue the criminal enquiry separately once they had established which section would be dealing with it.
- The Leaving Care Team stated that the plan was still for Peter to remain in his current placement until his eighteenth birthday.

Outcome

One month later the police received information that Peter had returned to the foster carer's home with his computer. They obtained a warrant and seized the computer.

- A joint interview between the police and social care took place.
- Peter denied any knowledge of the images.
- The police informed social care that forensic examination of the computer would take six months.
- Peter remained in foster care until his eighteenth birthday, which was one month after the seizure of the computer. After his birthday he did not go into semi-independent accommodation but went to stay with his father in another local authority area.
- The case was closed by social care.

What was actually going on?

Peter and his father have been sexually abusing Donna at Mr Raymond's house. They have been filming the abuse and sharing and swapping the videos with a loose network of individuals known to Mr Raymond.

How might this have been recognised?

Clear lines of reporting would have enabled a co-ordinated approach which would have addressed both the criminal aspects of the case with regard to the child abuse images and the wider child protection issues.

- The fostering agency should have contacted social care and the police as soon as they received the referral.
- In the first instance social care should have involved the LSCB e-safety lead officer, who ought to have the knowledge and experience to get the right agencies involved in the case.
- The LSCB e-safety lead officer should have thorough knowledge of local police arrangements and a working relationship with the teams that deal with internet-based child abuse.
- Similarly the local police should have arrangements with the LSCB to enable multi-agency working on cases of this type.

If these clear lines of reporting had been in place, consideration would have been given to the fact that the making, distribution and viewing of child abuse images is instrumental in the ongoing sexual abuse of children within organised abuse. Had further consideration been given to these additional risks and possibilities posed by the role played by ICT in the case, the scope of the investigation might have been widened.

For example:

- Consideration should have been given to the provenance of the videos and images. Had he downloaded them from a website or was Peter involved in paedophile newsgroups or peer-to-peer file sharing? The latter could indicate involvement in organised abuse.
- Possession of child abuse images could indicate contact offending. Questions may therefore have been raised about Peter's access to children and whether he was producing images himself.
- Peter's access to his sister, Donna, should have been considered. Her social worker should have been involved.
- Child abuse images may play a role in the grooming process. Consideration should have been given to contacts Peter may have been making both in the real and the virtual world.
- Police and agency checks should have been made with Mr Raymond's local constabulary and social services.
- If local police needed help, they should have contacted CEOP for guidance and support.

Case study 2

Report of abuse – a potential scenario

After attending an internet safety awareness session run by the LSCB, a teacher in a secondary school gives a PHSE lesson to their Year 9 class on the risks posed by predatory adults online. During the class a girl is visibly distressed by what is being discussed. Afterwards the teacher approaches her and asks if anything is wrong. The girl is reluctant to discuss anything but the teacher suspects that something is amiss.

The teacher approaches the designated child protection teacher, who is also the school's e-safety lead, and tells her about the girl's demeanour during the class. The child protection teacher decides to speak to the girl to give her a second opportunity to talk about the issues raised in the class. Though initially hesitant, the girl confides that she had been communicating online with a man for several months. She stated that their conversations had become increasingly sexual and, although she had initially gone along with this, she had become more and more uncomfortable. Despite this he persuaded her to strip for him on webcam. She had tried to stop communicating with him but he told her that he had recorded her undressing and he would post it on the internet if she didn't stay in contact.

The child protection teacher discussed this with the headteacher. The headteacher then spoke to the local authority child protection advisor for education, who was also a member of the LSCB e-safety subgroup. He advised the head to make a referral to social care. On receiving the referral, a social worker went to the school to conduct a joint interview of the girl with the police. After the girl had repeated her allegation of abuse to them, the police began an investigation, preserving any evidence held on the girl's computer which might be taken for later forensic examination.

Social care convened an urgent strategy meeting attended by representatives from social care, school and the police, as well the child protection advisor for education, who was also there to advise on e-safety issues. The strategy meeting considered whether the girl was in any immediate danger and laid out a plan for the investigation which was conducted jointly between social care and the police.

Case study 3

Cyberbullying – a potential scenario

A Year 9 pupil confides to the school nurse that she is being picked on. When asked to elaborate, the girl reveals that a group of girls has posted a video on YouTube of her at a sleepover dancing around in her pyjamas and singing into a hairbrush. They have added a soundtrack which makes it even more embarrassing. Apparently people all over the school have seen the video and she says that she can't walk down the school corridor without someone making a comment like "Nice pyjamas," or mimicking her in the video.

The nurse has attended e-safety awareness training run by the local safeguarding children board and is aware of the issues of cyberbullying. The nurse asks the girl if the other girls had done anything else which had upset her. The girl replied that they had also blocked her from their buddy lists on Instant Messenger and left hurtful comments about the video on her Bebo profile.

After reassuring the girl that she had done the right thing in reporting this, the school nurse informed the headteacher. The headteacher recorded the details and, following the school's anti-bullying policy, opened an investigation, making reference to the DCSF guidance on cyberbullying. The girls who had uploaded the video were identified and sanctions were applied. They were spoken to about the impact of such misuse of the internet and they removed the video from the video-sharing site. As they were identified and co-operative, there was no need to contact the video-sharing site to flag it as inappropriate content and ask for it to be removed.

Becta leading next generation learning

Sample LSCB e-safety strategy and action plan

1 LSCB e-Safety Strategy Group

2 Policies, procedures and practices

3 Education, training and information

4 Infrastructure and technology

5 Inspection and standards

G

Sample LSCB e-safety strategy and action plan

Introduction

The Leicester, Leicestershire and Rutland Local Safeguarding Children Board takes seriously the statutory role it has to ensure that member agencies co-operate to safeguard and promote the welfare of children and young people in the locality, and to ensure that they are effective in doing so.

As part of promoting the welfare of children and young people in accordance with the *Children Act 2004* and *Working together to safeguard children 2006*, the LSCB has devised an e-safety strategy plus a policy that is built on four key areas:

1. Policies, practices and procedures
2. Education and training
3. Infrastructure and technology
4. Standards and inspection.

The LSCB will be looking to member agencies for their support and co-operation in developing an environment where children and young people can use the internet and other digital technologies safely.

1 LSCB E-safety Strategy Group

Objectives

1.1 To decide and agree where the E-safety Strategy Group will sit within the organisational structure of the LSCB

1.2 To develop a position statement that will inform the overall strategy of the LSCB

1.3 To develop terms of reference for the E-safety Strategy Group and agree its membership, as well as clear roles, responsibilities and the nature of the accountability that the Strategy Group will have to the LSCB

1.4 To identify priority areas of action and associated funding

2 Policies, procedures and practices

Objectives

2.1 To ensure that member agencies and partners of the LSCB, as well as other settings in which children and young people access the internet and other digital technologies, have in place policies, procedures and practices that enable children and young people to use the internet and mobile digital technologies safely

2.2 To update and expand on the existing LSCB practice guidance (Chapter 12) related to internet safety

2.3 To clarify the reporting mechanism for all member agencies and partners of the LSCB and to make it inclusive of the Internet Watch Foundation and CEOP as well as the police

2.4 To develop a media strategy for dealing with child protection incidents

3 Education, training and information

Objectives

3.1 To audit the provision of e-safety training carried out and e-safety awareness campaigns by member agencies and partners with a view to obtaining consistency

3.2 In conjunction with the LSCB Training Sub-Committee, to develop an education and training strategy that will ensure the provision of education to children and young people that promotes safe and responsible use of the internet and other digital technologies. In addition, the strategy will include training for members of the children's workforce with a view to raising their awareness of e-safety and how it relates to safeguarding children

3.3 In conjunction with the Communications Sub-Committee, to develop an awareness campaign that will focus on educating key stakeholders (parents and carers, the media and partner agencies) about the opportunities and the threats of the internet and digital technologies

4 Infrastructure and technology

Objectives

4.1 To develop for member agencies and partners of the LSCB a set of robust principles and guidance about safe internet provision that take into account national standards on filtering and accreditation of software

4.2 To develop and disseminate good practice information to other providers (such as post offices, internet cafés, phone boxes, digital handheld devices and mobile phones) aimed at enabling children and young people to use the internet safely and responsibly

4.3 To develop a mechanism that will bring together experts in ICT and related technologies and also practitioners with a statutory duty to safeguard children to consider new and emerging technologies and their trends, and to disseminate good practice as quickly as possible to agencies providing services to children, young people and their families

5 Inspection and standards

Objectives

5.1 To develop an e-safety monitoring dataset, which member agencies can report on, and which includes policies, practices and procedures; organisational internet safety reporting mechanisms; infrastructure arrangements and training

5.2 To develop a monitoring mechanism that will record the national standards on internet safety to which member agencies adhere

5.3 In conjunction with the Quality Assurance Sub-Committee, to develop a number of themed audits that identify the extent to which e-safety is embedded as part of the safeguarding responsibilities of member agencies and partners of the LSCB

5.4 In conjunction with various forums for children and young people, to develop a mechanism that collates their views and opinions on the safeguarding practices related to e-safety

Key area	Objectives	Action required	Responsibility of	Expected completion date
1. LSCB E-safety Strategy Group	1.1 To decide and agree where the E-safety Group will sit within the organisational structure of LSCB 1.2 To develop a position statement that will inform the overall strategy of the LSCB 1.3 To develop terms of reference for the E-safety Strategy Group and agree its membership, as well as clear roles, responsibilities and the nature of the accountability that the Strategy Group will have to the LSCB 1.4 To identify priority areas of action and associated funding	• Organise a half-day meeting for members of the LSCB E-safety Working Group to decide on organisational issues, develop a position statement, develop terms of reference, clarify roles and responsibilities, set out the nature of the accountability that the Strategy Group will have to the LSCB and identify the priority areas for action and associated funding • Write a paper for the Core Business Group which will put forward a position statement, terms of reference, membership, roles and responsibilities, nature of accountability and priority areas for action by the Strategy Group		
2. Policies, procedures and practices	2.1 To ensure that member agencies and partners of the LSCB, as well as other settings in which children and young people access the internet and other digital technologies, have in place policies, procedures and practices that enable children and young people to use the internet and mobile digital technologies safely	• Conduct an audit exercise which includes an action plan across all member agencies of the LSCB and key partners to identify any gaps in policies, procedures and practices		

Key area	Objectives	Action required	Responsibility of	Expected completion date
2. Policies, procedures and practices	2.2 To update and expand on the existing LSCB practice guidance (Chapter 12) related to internet safety	• Identify members of the E-safety Strategy Group to review the practice guidance • LSCB Policy Officer to obtain a number of practice guidance publications from other LSCBs and identify key issues in *Working together to safeguard children 2006* as background material for the new practice guidance • Draft practice guidance and distribute for consultation via the Development Sub-Committee • Re-draft practice guidance as a result of the consultation exercise and then forward to LSCB for ratification		
	2.3 To clarify the reporting mechanism for all member agencies and partners of the LSCB and to make it inclusive of the Internet Watch Foundation and CEOP as well as the police	• Hold meeting between RBC, police and other key agencies to agree an internet safety reporting mechanism • Draft in writing the internet safety reporting mechanism • Complete a consultation exercise which includes the IWF and CEOP • Disseminate internet safety reporting mechanism across LSCB member agencies and partners		
	2.4 To develop a media strategy for dealing with child protection incidents	• Identify and develop existing procedures in order to deal with child protection concerns relating to the internet and other digital technologies		

Key area	Objectives	Action required	Responsibility of	Expected completion date
3. Education, training and information	3.1 To audit the provision of e-safety training carried out and e-safety awareness campaigns by member agencies and partners with a view to obtaining consistency	• Approach Chair of Quality Assurance Sub-Committee, requesting that the Performance and Review Officer undertake an exercise to collate details of what e-safety training member agencies carry out		
	3.2 In conjunction with the LSCB Training Sub-Committee, to develop an education and training strategy that will ensure the provision of education to children and young people that promotes safe and responsible use of the internet and other digital technologies. In addition, the strategy will include training for members of the children's workforce with a view to raising their awareness of e-safety and how it relates to safeguarding children	• Hold meeting between Chair of E-safety Strategy Group and LSCB Training Sub-Committee to formally request a small working group to: 1 Identify key individuals for the working group, agree activities that are to be completed such as education and training for children and young people, as well as a strategy for training members of the children's workforce (level of training, programme of training to be implemented) 2 Report back to E-safety Strategy Group with a suggested strategy, action plan and costings and then report back		

Key area	Objectives	Action required	Responsibility of	Expected completion date
3. Education, training and information	3.3 In conjunction with the Communications Sub-Committee, to develop an awareness campaign that will focus on educating key stakeholders (parents and carer, the media and partner agencies) about the opportunities and the threats of the internet and digital technologies	• Hold meeting between Chair of E-safety Strategy Group and LSCB Communications Sub-Committee to formally request a working group to look at an awareness campaign for parents and carers, the media and artner agencies • Identify key individuals for working group and agree activities to be completed such as creating a leaflet or additional material for the LSCB website • Report back to E-safety Strategy Group with a suggested strategy, action plan and costings		
4. Infrastructure and technology	4.1 To develop for member agencies and partners of the LSCB a set of robust principles and guidance about safe internet provision that take into account national standards on filtering and accreditation of software	• Set up a small working group, which includes representatives of the RBC and other agencies, to develop a set of ISP provisions that are in accordance with national and regional standards • Draft provisions and consult on them with key agencies • Re-draft provisions and present formally to E-safety Strategy Group, which will then forward them to the LSCB for ratification, with a view to incorporating them into 2.2 guidance		

Key area	Objectives	Action required	Responsibility of	Expected completion date
4. Infrastructure and technology	4.2 To develop and disseminate good practice information to other providers, aimed at enabling children and young people to use the internet safely and responsibly 4.3 To develop a mechanism that will bring together experts in ICT and related technologies and also practitioners with a statutory duty to safeguard children to consider new and emerging technologies and their trends, and to disseminate good practice as quickly as possible to agencies providing services to children, young people and their families	• Develop an action plan that will identify other providers and the nature, level and frequency of discussions that are required • Disseminate information to providers • Develop a mechanism that will harness information and guidance regarding the latest developments in internet and digital communication; also disseminate the information speedily to member agencies and other providers • Identify a key person responsible for developing and maintaining the mechanism		
5. Inspection and standards	5.1 To develop an e-safety monitoring dataset, which member agencies can report on, and which includes policies, practices and procedures; organisational internet safety reporting mechanisms; infrastructure arrangements and training	• Hold meeting between Chair of E-safety Strategy Group and QA Sub-Committee to formally request a working group to look at the development of a dataset • Identify key individuals for the working group and agree activities to be completed such as producing draft of a dataset, possible consultation exercise and so on • Report back to E-safety Strategy Group with a mechanism for distributing the dataset, collating and analysing the information concerned and then disseminating good practice		

Key area	Objectives	Action required	Responsibility of	Expected completion date
5. Inspection and standards	5.2 To develop a monitoring mechanism that will record the national standards on internet safety to which member agencies adhere	• Approach Chair of QA Sub-Committee about having the Practice and Performance Review Officer develop a tool that will allow all agencies to keep formal records of the standards to which they adhere • Report by the Practice and Performance Review Officer to E-safety Strategy Group on the development and execution of the tool devised and the results		
	5.3 In conjunction with the Quality Assurance Sub-Committee, to develop a number of themed audits that identify the extent to which e-safety is embedded as part of the safeguarding responsibilities of member agencies and partners of the LSCB	• Approach Chair of QA Sub-Committee regarding the development and execution of a number of themed audits • Reports to E-safety Strategy Group of themed audits undertaken		
	5.4 In conjunction with various children and young people's forums, to develop a mechanism that collates their views and opinions on the safeguarding practices related to e-safety	• Map the consultation forums that exist for children and young people across Leicester, Leicestershire and Rutland • Identify key forums in conjunction with the Practice and Performance Review Officer and then develop feedback response mechanism • Report back to the E-safety Strategy Group the results, which then feed into the Group's strategy and action plan for the following year		

Becta leading next generation learning

Participants in the Becta e-safety working days

Acknowledgements

Acknowledgements

Becta would like to thank the following organisations for their contributions to the Becta e-safety working days in September 2007, for sharing their e-safety resources, and for their continued support in the writing and production of this publication.

- Birmingham City Council
- Blackburn with Darwen Borough Council
- Cambridgeshire County Council
- Cumbria County Council
- Derby City Council
- Devon County Council
- Dudley Metropolitan Borough Council
- Essex County Council
- European Schoolnet
- Gloucestershire County Council
- Hartlepool Borough Council
- Herefordshire County Council
- Kent County Council
- Kirklees Council
- Knowsley Metropolitan Borough Council
- Learning and Teaching Scotland
- Leeds City Council
- Leicester City Council
- Leicestershire County Council
- Liverpool City Council
- London Borough of Brent
- London Borough of Harrow Council
- London Borough of Havering
- London Borough of Islington Council
- London Grid for Learning
- Luton Borough Council
- National Assembly for Wales
- North Tyneside Metropolitan Borough Council

- Northamptonshire County Council
- Northern Grid for Learning
- Royal Borough of Kensington and Chelsea
- Sandwell Metropolitan Borough Council
- Sheffield City Council
- Shropshire County Council
- Solihull Metropolitan Borough Council
- South West Grid for Learning
- Staffordshire County Council
- Stockport Metropolitan Borough Council
- Tameside Metropolitan Borough Council
- Telford and Wrekin Council
- Walsall Metropolitan Borough Council
- Warwickshire County Council
- West Midlands Regional Broadband Consortium
- Wiltshire County Council
- Worcestershire County Council
- Yorkshire and Humber Grid for Learning

Thanks also go to all the individuals and organisations that kindly provided feedback during the draft stages of this publication and to those organisations that have granted permission for us to reproduce or reference their logos or resources.

Becta leading next generation learning

Millburn Hill Road
Science Park
Coventry CV4 7JJ

Tel: 024 7641 6994
Fax: 024 7641 1418
Email: becta@becta.org.uk

www.becta.org.uk

01/DD07-08/162/MP/2k