E-SAFETY POLICY

JUNE 2015

Contents

	Page
Introduction	**4**
Definition of E-safety	**4**
Our Vision	**4**
Background	**5**
Risks	**5**
Forms of abuse through Internet Digital Mobile Technology	**7**
Why do we need an e-safety policy?	**7**
Stakeholders	**8**
Objectives	**8**
Objective 1: Ensuring that all children, young people & parents/carers should be equipped with the knowledge and skills to safeguard themselves in the online/digital world.	**9**
1.1 – E-safety education	**9**
Objective 2: Ensure that all people who work with children and young people have access to effective policies and procedures and effective training to safeguarding children at risk through online activity.	**10**
2.1 – Developing filtering standards	**11**

2.2 – Email	**12**
2.3 – Mobile Phone	**13**
2.4 – Social Networking	**13**
2.5 – Web Cameras	**15**
2.6 – Gaming	**15**
2.7 – Cyber-bullying	**15**
2.8 – Publishing young people's images and work	**16**
2.9 – Illegal downloading	**16**
Objective 3: Ensure that professional know how to respond when concerns arise regarding the misuse of communications technology.	**17**
3.1 – E-safety complaints	**17**
3.2 – Monitoring e-safety incidents and reporting abuse	**17**
3.3 – Promoting the policy	**18**
3.4 – Staff engagement	**18**
3.5 – How do we respond?	**19**
Committing an illegal Act – Did you know?	**20**
What to do with suspicious email received at work	**21**

Appendix 1 – Glossary	**28**
Appendix 2 – Notes on the legal framework	**32**
Appendix 3 – Sources of External ICT Support	**38**

Introduction

Essex Safeguarding Children Board (ESCB) recognises e-safety issues and the potential harm and risks it can pose to children and young people. All partner agencies, stakeholders, schools and educational settings and all other organisations within the community providing services to children have a duty to understand e-safety issues as part of its wider safeguarding duties; recognising their role in helping children to remain safe online while also supporting the adults who care for children. ESCB acknowledges that its role is strategic rather than operational as it is for partner agencies to develop and embed their own operational policies and procedures, and lines of accountability, in safeguarding children when using Internet, Digital and Mobile Technologies (IDMT). This policy needs to be read in conjunction with the SET procedures and it is envisaged, that this document will provide a framework for partner agencies in this regard in line with the following definition of e-safety and our ESCB vision.

Definition of e-safety

The term e-safety is defined for the purposes of this document as the process of limiting the risks to children and young people when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection (source BECTA. BECTA was closed by the coalition government 31st March 2011).

Essex Safeguarding Children Board's Vision

Our vision is that all children and young people, all parents/carers and foster carers and all those working with children and young people recognise the risks, dangers and potential harm that may arise from the use of Internet Digital and Mobile Technologies, that they understand how to mitigate these risks and potential dangers and are able to recognise, challenge and respond appropriately to any e-safety concerns so that children and young people are kept safe.

Background

Article 17 of the United Nations Convention on Rights of the Child (UNCRC) states that, "Children have the right to get information that is important to their health and well-being. Governments should encourage mass media - radio, television, newspaper and internet content sources - to provide information that children can understand and to not promote materials that could harm children."
The Sexual Offences Act 2003[1] includes a number of offences related to child abuse online.

ESCB is aware that the understanding and use of Internet, Digital and Mobile Technology (IDMT) is essential to helping and encouraging every child to reach their full potential. As the Board we have to raise awareness and educate those involved in children's welfare and development about the dangers that children and young people can face in the online world, whilst accepting that safety in the online world is not the removal or banning of access to digital technologies in itself but rather education and training, for both children and adults, around responsible use and potential dangers.

All organisations providing services for children and young people have a responsibility to ensure that they understand e-safety issues, know how to help children stay safe online and have procedures in place to support those working with children in knowing how to respond when concerns arise.

Risks

Children and young people do not always recognise the inherent dangers of the internet and often do not understand that online behaviour may have offline consequences.

Despite this, digital technologies can offer them opportunities to learn and develop, communicate, be creative and be entertained. The advantages of the internet can and should out-weigh the disadvantages.

However, we now have a greater understanding to the extent of the risks the digital world can pose to children.

[1] www.homeoffice.gov.uk/documents/adults-safe-fr-sex-harm-leaflet

Risks include:

The Byron review classifies the risks inherent in the use of new technologies as relating to content, contact and conduct. The risk is often determined by behaviours rather than the technologies themselves:

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

Byron review of Children and new technology (2008) Published by DCSF and DCMS

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse.

Contact

- Grooming using communication technologies to meet and groom children with the intention of sexually abusing them (both on and off line exploitation).

Commerce/Conduct

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

BECTA (2007) identify some of the issues which are summarised below.

Forms of Abuse through Internet Digital and Mobile Technologies (IDMT)

- Children and young people have been 'groomed' online by adults (often pretending to be those who care) with the ultimate aim of exploiting them sexually.
- Children / young people have been bullied by other young people via social networking sites, websites, instant messaging and text messages; this is often known as 'cyber-bullying'.
- Inappropriate (i.e. threatening, indecent or pornographic) images of children and young people have been taken, uploaded and circulated via social network websites, mobile telephones and video broadcasting websites such as You Tube, often by other young people. This is a criminal offence under s45 of the Sexual Offences Act 2003.
- The dangers attached to gang culture can rapidly accelerate online as many gangs 'advertise' or promote themselves via websites or social networking sites or if threats of violence, threats to an individual's life or threats of retaliation are posted online by opposing gang members.
- Unsuitable websites and images can easily be accessed online.
- Images of physical abuse, crime, racism, self-harm, terrorism or on physical violence to influence young minds.

Ignoring the dangers that children / young people can face would lead to serious gaps in our responsibilities towards safeguarding and child protection.

Why do we need an e-safety policy?

Each new technology introduces new opportunities and challenges for children and young people, parents, carers and those working with young people. In order to minimise the risks involved from new technologies we need to understand how children and young people use IDMT and how this may be misused by those who may present a risk to children. It is important that we know how to respond when concerns arise.

In recent years the internet and other means of electronic communications have become increasingly accessible to children and young people. This provides great opportunities for young people in terms of education, information, communication and having fun. However, it also includes risks from those intent on sexually exploiting children and from the inappropriate use of communications technology. This highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It also highlights the need to provide appropriate guidance to those working with children and parents and carers.

Local Safeguarding Children Boards have an important role in co-coordinating and ensuring the effectiveness of local work to safeguard and promote the welfare of children. This document aims to support organisations in reviewing their own e-safety agenda and to help in developing effective e-safety policies and procedures.

Stakeholders

Statutory and voluntary organisations that children and young people and families may use should consider having an e-safety policy. These include community groups and private sector organisations also.

This document aims to provide information for organisations in helping them to develop e-safety policies.

Objectives

All organisations that work with children and young people need to have an e-policy in place based on the following objectives:

1. ***Ensuring*** *that all children, young people, parents/carers and foster carers should be equipped with the knowledge and skills to safeguard themselves in the online/digital world;*

2. ***Ensuring*** *that all people who work with children & young people have access to effective policies and procedures and effective training to safeguard children at risk through online activity; and*

3. ***Ensuring*** *that professionals know how to respond when concerns arise regarding the misuse of communications technology.*

Objective 1: *Ensuring that all children, young people, parents/carers and foster carers should be equipped with the knowledge and skills to safeguard themselves in the online/digital world;*

As Internet Digital and Mobile Technologies are constantly changing there is information available to help children and young people stay safe on line, the following sites may help in developing an e safety policy:

www.thinkuknow.co.uk and www.ceop.co.uk
The Child Exploitation and Online protection (CEOP) centre delivers a multi-agency service dedicated to tackling and bringing offenders to account either directly or with local and international police forces and working with children and parents to deliver their ThinkuKnow internet safety programme.

http://www.iwf.org.uk/
The Internet Watch Foundation was established in 1996 by UK internet industry to provide an internet hotline for public and IT professionals to report potentially illegal online content with the intention of having the offending material removed.

www.pitda.co.uk
Parenting in the digital age

NSPCC Share aware campaign and materials

1.1 E-safety education

1. Children and young people need to be educated in the responsible and safe use of the Internet and other technologies through a range of strategies.

2. Organisations providing internet access to children / young people (schools, libraries, youth clubs etc.) must ensure that they do so in a way that is safe and age appropriate for children / young people by way of appropriate filtering systems etc.

3. Young people must be made aware that perpetrators who forward indecent images could be prosecuted under s45 of the Sexual Offences Act 2003 for the distribution of child pornography which may result in them being registered on the Sex Offenders Register if convicted.

4. Children and young people should be advised that not all information is true but can be misleading and derogatory.

5. Children and young people need to be made aware that they may encounter content on IDMT that distorts and misrepresents what constitutes a good and safe relationship.

6. Designated e-safety champions and leads should register with websites such as Ofcom in order to keep up to date with new digital technologies. www.ofcom.org.uk

   Websites:
   www.ceop.gov.uk
   www.thinkuknow.co.uk/parents

Objective 2: *Ensuring that all people who work with children & young people have access to effective policies and procedures and effective training to safeguard children at risk through online activity*

The Internet Digital and Mobile Technologies are constantly developing and evolving and this section is only intended to give an idea of the range of communications channels used by people to contact each other and exchange electronic data - including Child abuse images.

Security is a complex matter and queries should always be referred directly to the responsible body relevant to the agency.

Employees and service users (including young people) should be aware that abuse of recognised policies and procedures could result in a withdrawal of technology provision and potential legal / disciplinary action being instigated against the perpetrator.

All users must be compliant to an Acceptable Use Policy (AUP) for example:

- not act un-reasonably and be inconsiderate of other service users.
- must take responsibility for their own network use
- Computer and internet access should have appropriate security and anti-virus protection.
- Must ensure to not disable or circumvent security measures – filters, encryption etc.

- Must not have personal and sensitive electronic data taken offsite without being security encrypted and authorised by management.
- Must not have unapproved software being introduced into local networks and not authorised by management.

2.1 Developing filtering standards

- It is important to use as a minimum an ISP who subscribes to the Internet Watch Foundation (IWF) filtering list. This will help to filter out some inappropriate content, but not all. Using an accredited Internet Service Provider (ISP) will also provide higher standards for filtering.
- Levels of internet access and supervision must be age appropriate and suitable for the young people. Filtering systems should be secure but adaptable.
- Older children and professionals may sometimes require temporary access to a normally restricted website in order to carry out research for a project or study. Providing this can be justified by management, restrictions may be temporarily removed however access should be monitored.

Access controls (filtering) fall into several overlapping types:

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- An “allow list” restricts access to a list of approved sites. Such lists inevitably limit young people’s access to a narrow range of information.
- Dynamic filtering examines web page content or email for unsuitable words. Filtering of outgoing information such as web searches is also required.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
- Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.
- Management should ensure that regular checks are made to ensure that filtering methods selected are age appropriate, effective and reasonable. Access to inappropriate websites any material perceived to be illegal must be reported to management who should inform this to the appropriate agency.

2.2 Email

- Email is now an essential means of communication which can also be accessible via most mobile phones. A degree of responsibility has to sit with children, young people and professionals since as soon as email access is permitted it is very difficult to control. Restricting both incoming and outgoing email to specific addresses is possible, however, not always practical as addresses can easily be changed. Microsoft Office 365 mail used by most organisations is scanned and filtered for spam and has an editable abusive language filter.
- Email should not automatically be considered private and most organisations reserve the right to monitor email. However, there has to be a balance between maintaining the safety of children / young people and their rights to privacy, which are covered by legislation.
- Email content and tone must also be considered. Due to the impersonal nature of email, children and young people may write things or be aggressive or dismissive in tone which may be hurtful to others, even if such content or tone is not intended it may still be considered as cyber-bullying.
- Young people should also be encouraged to be creative and non-identifiable in setting up personal email addresses.

General guidance includes:

- Children / young people should not reveal personal information about themselves or other young people via email nor ever arrange to meet strangers by email without specific permission from an adult in authority and this should always be under supervision and preferably in a public place.
- Where possible, organisations such as education settings should consider the use of learning platforms and generic email accounts where students are required to submit coursework rather than by pupil to teacher's personal accounts.
- Organisations should always prohibit the forwarding of chain emails.
- Professionals should only communicate with young people by email if this has been agreed in advance with the child / young person, their parent/carer/foster carer and management and via equipment owned by their employer.
- It is a Professionals' responsibility if they have disclosed their personal email addresses to children / young people.
- Children / young people should advise a responsible adult or lead person if they receive offensive or threatening email.

2.3 Mobile Devices

Most young people now have access to mobile telephones which are generally perceived as essential to their day to day living and communicating and now offer access to the internet, instant messaging, email, social networking, a camera and video facilities. Mobile phones are becoming the most commonly used tool for internet access and social networking for young people. Mobile phones therefore pose one of the biggest online threats to young people as they allow instant access to all forms of IDMT.

- Children / young people and adults should be made aware to only share telephone numbers with those known to them and ensure that electronic records (call, text and email logs) are kept of any bullying or threatening telephone calls, text messages, emails or images received which may need to be used as evidence in any police investigation.
- Children / young people should be careful about accepting invitations to join location based social networking sites such as GyPSii that allow your location to be identified via GPS enabled phones.
- Schools and education settings and early years settings may restrict the use of mobile devices during working hours. **Similar restrictions must apply to parents and carers when they are in the premises of the educational / early years and childcare setting.**
- However, in some settings permitting responsible use of the mobile phone in conjunction with a cyber-bullying education programme is also an approach.
- Scrutiny of the content of a pupil's mobile phone by a school or an alternative education provision (AEP) is not an automatic right and schools and AEP's must clearly outline in their policies that they have the authority to do so under the Education Inspections Act 2006 and specify the circumstances under which this may happen. It is usual for this to be cited in their policies.

2.4 Social Networking

The Internet provides ready access to online spaces and social networking sites which allow individuals to publish un-moderated content. Social networking sites such as Facebook, Twitter, Chat Rooms, Online Gaming Platforms and Instant Messaging can connect individuals to groups of people which may be friends in the 'virtual' world but who may have never met each other in the real world. Users can be invited to join groups and leave comments over which there may be limited or no control.

Children / young people should be encouraged to consider the associated risks and dangers related to sending or accepting friend requests and posting personal comments, inappropriate images or videos about themselves or their peers and the subsequent difficulty in removing an inappropriate image or information once published. They should also be advised not to publish detailed private thoughts or emotions which could be considered threatening, intimidating or hurtful to others.

Children / young people should also be encouraged to never give out any personal details or images which may identify themselves, their peers, their siblings / foster siblings, their location or any groups, schools or organisations they attend or associate with. This includes real names, dates of birth, address, phone numbers, e-mail addresses, photographs or videos, school attended, IM and email addresses, including those of friends, family / foster family and peers. This also includes any 'gangs' they may be affiliated with.

Children / young people must be advised about e-security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. They should be encouraged to invite known friends only and deny access to others by making their profiles private and only accept friend requests from those already known to them.

Care should be taken to delete old and unused profiles from websites which are no longer used as these will remain accessible to others. Personal information voluntarily shared by a young person is unlikely to remain the same as the person matures and has a greater understanding of how personal information about them can impact on their later lives (i.e. perspective employers making an online search of their name and sighting inappropriate photographs, videos or content etc.).

Professionals working or in a position of trust with children / young people (including volunteers) must also familiarise themselves about the risks and inappropriateness of sharing personal information about themselves via social networking sites with young people. They should be made aware that any inappropriate material posted could affect their professional status.

Professionals must responsibly restrict access to their friends and family only and 'friend requests' by a young person may be within professional boundaries.

Professionals must also steer clear of social networking sites that young people are known to frequent except in certain roles.

2.5 Web Cam

It is now generally accepted that the term “child pornography” should not be used, because it conflates the images of child abuse (which constitute “child pornography”) with adult pornography which may be perfectly legal. There are different opinions about this, but it has now become generally accepted that the term “child sexual abuse images” is more appropriate, and most agencies have adopted this practice in their written material.

Individuals caught in possession of child abusive images will nearly always arise as a result of a police investigation and the seizure of images, possession of which is an offence under the Protection of Children Act 1978 – amended 1994. This states:

“It is an offence for a person….
a) …. to take, or permit to be taken, or to make, any indecent photographs or pseudo- photographs of a child
b) …. to distribute or show such indecent photographs or pseudo-photographs.”

2.6 Multi-player games on line

Children, young people and responsible adults need to understand that their online behaviour may have consequences as although it’s an online game the players are real people**.**

2.7 Cyber-bullying

Cyber-bullying can be defined as “*The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone*” (DCSF 2007).

Children / young people should find using IDMT as a positive and creative part of their everyday life. Unfortunately, IDMT can also be used negatively to target a specific young person or group.

- It should also be noted that professionals, especially teachers and other education staff are particularly vulnerable to ‘cyber-bullying’ by pupils or even ex-pupils, which may include general insults, threats, harassment, defamation, homophobic or racist remarks or other forms of prejudice based bullying. The effects of cyber bullying by young people on adults are equally distressing and the impact on the victim can be just as profound – Government guidance notes remind us that cyber bullying incidents are upsetting whoever the victim is and whatever age they are.

- Employers should be alert to the possibility and potential for cyber bullying towards members of staff by young people and appreciate there is no single solution to the problem.
- Instances of cyber-bullying must be responded to sensitively and in line with existing anti-bullying policies and procedures in the organisation.
- The victim of cyber-bullying must be reassured they have done the right thing in disclosing the bullying and be supported. Please refer to the attached **Appendix** for further information on this. This should also be cross referenced with the local anti-bullying policy.

2.8 Publishing young people's images and work

- Many organisations create websites inspired by pieces of work and quotations and statements from young people. Often these can include images or videos of young service users which help promote and make the organisation identifiable to other young people. Still and moving images and sounds can add liveliness and interest to a publication, particularly when young people are included nevertheless the security of children / young people is paramount and names and identifiable locations of young people should never be linked to their images. (For example, a child placed in a refuge for domestic violence could be traced back to a school by their school uniform).
- Children / young people should also be advised when photographs or video footage of them is being taken and images should never be published without the consent of the young person, and the written consent of their parent/carer or foster carer.
- Although it is fairly simple to upload comments, images and videos on social networking and video broadcasting websites, young people must be encouraged to consider the associated consequential risks and dangers in doing this and the difficulties in removing this content, particularly if the content subsequently becomes the property of the publisher.
- Inappropriate offensive, pornographic or threatening content can have devastating consequences to individuals and groups (including gangs) and young people should be made aware of the legalities and long term implications of doing this.

2.9 Illegal Downloading

Whilst there are many sites where music, videos and software can be legally downloaded, children young people and adults need to be made aware that they could be breaking the law by downloading copyright protected files or by infringing other intellectual property rights.

The various industries affected by illegal downloading (particularly music) do monitor the internet and can take legal action ranging from fines to suing those who hold parental responsibility. It is recommended that websites are thoroughly researched prior to downloading content for personal use.

Objective 3: *Ensure that Professionals know how to respond when concerns arise regarding the misuse of communications technology.*

3.1 e–safety complaints

- Any complaints about e-safety concerns should be progressed via the organisations recognised complaints procedure which should be readily accessible to all; however efforts should be made to resolve low level issues internally. These must be recorded locally. See the flow chart.
- All factors in relation to the complaint must be clearly established in order to have substance.
- Complaints about employee's IDMT misuse should be escalated to the most senior manager within the organisation and be managed according to recognised disciplinary and child protection procedures.
- Employers must have internal methods of scrutinising IDMT use, in particular, the ability to identify sites accessed. This is particularly important where there is an allegation that illegal or inappropriate websites have been accessed.
- Potentially illegal issues must always be referred to the police in the first instance.

3.2 Monitoring e safety incidents and reporting abuse

Any form of electronic or digital abuse towards young people should in the first instance be reported to the Child Exploitation Online Protection service www.ceop.police.uk, and also reported to the relevant IDMT lead with the organisation. Any incidents which place a young person in immediate danger should be referred to the local police by calling 999.

It is recommended that the CEOP 'report abuse' tool is downloaded onto all computer browsers.

This tool provides instant online access to report any form of online abuse. Young people should also be encouraged to download this tool directly onto their electronic devices, especially applications such as personal Facebook profiles.

Safeguarding Children Board seeks to ensure that partner agencies monitor the following as a suggested minimum dataset of e-Safety incidents:

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

3.3 Promoting the Policy

It is recommended that organisations include children and young people in the design and layout of their e-safety policy as their perceptions of risk will vary from age group to age group.

Ideally, posters should be displayed in rooms where computers can be accessed which highlight the policy and reiterate that all network and internet usage will be monitored and appropriate action will be taken if abuse occurs.

This policy should be made readily available to parents / carers and foster carers by way of being included and accessible on the organisations published literature and website.

3.4 Staff Engagement

- All staff with responsibility for young people's learning via IDMT must be familiarised with this policy and given opportunities to raise issues and concerns they face in their day to day working responsibilities.
- All staff must understand that misuse of IDMT will result in disciplinary action being taken against them in line with your organisations policies and procedures. Employees unsure of what constitutes acceptable usage of the internet should always check with management. They should be aware that all internet usage is monitored and can be traced back to each individual user.
- Staff must also be aware of what is acceptable in terms of their engagement with children and young people via IDMT means.
- Staff (including volunteers) should never disclose or share their personal details except in certain exceptional roles (i.e. personal mobile phone numbers, email addresses or social networking profiles etc.) or send or accept friend requests on social networking websites with children and young people / service users.

- Any necessary contact between a young person and a professional should be made via equipment and contact details provided by the employer (not personal equipment / contact details) and be clearly recorded on a need to communicate basis and with the consent of the parent/ carer or foster carer. Alternatively, personal contact details for children / young people should be stored centrally by management and only accessed on a need to know basis as approved by management.
- Organisations should adopt an open culture of vigilance in the workplace and staff must feel confident in identifying and challenging poor and/or risky working practices. For further guidance on Safer Working Practice with Technology, please refer to the supplementary guidance in **Appendix 3.** Ideally, training on acceptable usage and responsible e-safety should be provided during the induction period for all new employees with a specific emphasis on professional boundaries, confidentiality and data protection.
- This section will help staff determine what action they can take when they identify concerns and should be read in conjunction with the SET Procedures.

3.5 How do we respond?

The response required will depend on the nature of the incident. Concerns may relate to:

- The accidental access to inappropriate material
- Accidental access to illegal material
- Deliberate access to inappropriate material
- Inappropriate or illegal use of technologies
- Bullying or harassment using technology

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 possession of illegal material

4

Showing anyone else illegal material that you have received **is an illegal act**

5

Printing a copy of the offensive email to report it to someone else **is an illegal act** and is classed as producing 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

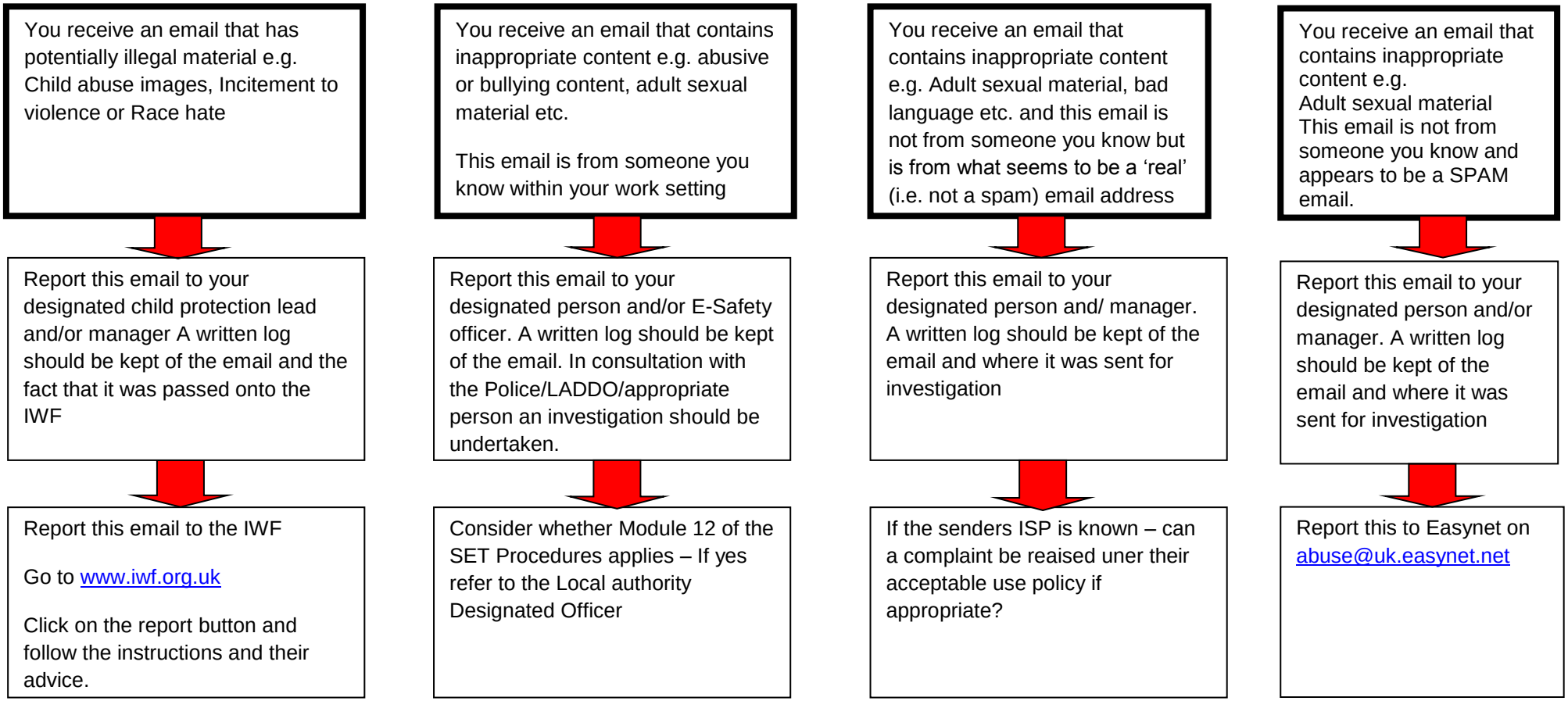
Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it

9

Always report potential illegal content to the Internet Watch Foundation at www.iwf.org.uk They are licensed to investigate **you are not.**

Never personally investigate. If you open illegal content accidentally report it to your manager and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, 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 237 700. **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.**

What to do with Suspicious Email received at work



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 manager and take the advice 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 other's email addresses. If you are unsure how to proceed please contact the Northern Grid for Learning on 0191 4611844

DEVELOPING AN E-SAFETY POLICY - BEST PRACTICE CHECKLIST

This checklist has been developed from "Safeguarding Children on line - a checklist for local authorities and LSCB's" BECTA. When completed it aims to give LSCB partners a snapshot of their e-safety issues and risks and to signpost activities that they need to develop across services. It is recommended for use in schools, youth centres, libraries and any services where children have access to technology and should be read in conjunction with the LSCB guidance on developing an e-safety policy.

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

Policies and practices

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

	In place y/n	Evidence attached	Areas for development
Does the organisation have an e-safety policy?			
Who is responsible for co-ordinating e-safety in the organisation to ensure that best practice is developed, implemented and kept up to date?			
Is there a regular risk assessment of your e-safety infrastructure?			
Do all services have acceptable use polices (AUP's) of IDMT by children, young people and staff? Have staff signed an acceptable use policy?			

	In place y/n	Evidence attached	Areas for development
Is the application of these policies monitored? *Are the AUPs kept up to date in line with changing issues and technologies?*			
Are the children and young people that use your services aware of their responsibilities for staying safe when online? Are they aware of their responsibilities to others? Do they know who to speak to if they encounter problems online or accidentally access inappropriate materials? *Consider links to "thinkuknow" website as a means of reporting*			
Is the privacy of children and young people protected when they are online? *e.g. if you include photographs of children on your website, for example, you will need to gain permission from the parents or guardian to use those images*.			
What are the procedures for reporting e-safety incidents of misuse? Are staff aware of their responsibilities in responding to certain types of incident? How are incidents escalated? *Do you pass information to the Internet Watch foundation?*			

Infrastructure and technology

	In place y/n	Evidence attached	Areas for development
Are there minimum standards for technical e-safety in all settings where children may access IDMT? *Do you have filtering systems in place to prevent access to inappropriate material?* *Are you using accredited ISPs?* *Becta's functional and technical specifications give further information.* *[**http://www.becta.org.uk/industry/techstandards**].*			
How are technical standards monitored? *Are local issues centrally reviewed for evidence of emerging problems or trends?*			

Communication and Training

	In place y/n	Evidence attached	Areas for development
How does your organisation seek to 'raise awareness about the safe use of the internet' – and other technologies? a)with children and young people b)with staff c)parents and carers			
Who co-ordinates activities in the 'development and delivery of training and education programmes with CEOP'?			
What is the organisation's strategy for educating and training staff in e-safety? Have your staff received e-safety awareness training? *This should include induction of new staff, plus ongoing support and supervision of existing staff. Staff should be aware of appropriate local, regional and national issues with regard to e-safety, and should be confident in their abilities to escalate an incident as necessary and appropriate.*			
Is existing good practice within Essex shared? *Many organisations may already have e-safety strategies in place. If you are interested in sharing your good practice, please send any materials to*			

	In place y/n	Evidence attached	Areas for development
the ESCB who will share these across other services.			
How are children with additional vulnerabilities safeguarded on line? *e.g: children and young people outside of mainstream education, children with disabilities*			
How will the impact of education and training be monitored and evaluated?			
What e-safety information and guidance is provided to parents and carers?	]		

Standards and inspection

	In place Y/N	Evidence attached	Areas for development
Who is responsible for monitoring e-safety measures? *As discussed in the policies and practices section, a responsible officer should take the lead in developing an e-safety agenda.*			
How is activity monitoring co-ordinated, particularly where several agencies have responsibility in this area? *Co-ordination is essential in order to incorporate recommendations and guidance from all agencies*			

involved in child protection into local e-safety policies and practices. Are emerging themes and trends passed to a central coordinator with your organisation?			
How is performance measured, and how is progress benchmarked? How is good practice shared? How is poor performance managed? Who drives forward recommendations?			

Appendix 1 - Glossary

Acceptable use: A policy that a user must agree to abide by policy (AUP) in order to gain access to a network or the internet. It may also cover how other communications devices, such as mobile phones and camera phones, can be used on the premises.

Adware: A program that appears to be free but may be paid for by companies whose products are advertised every time you use it. Some adware contains small programs that track the websites you visit on the internet, reporting the information back to marketing sites which then tailor advertisements to your interests. This is similar to spyware. The most sophisticated spyware can even track what keys you are hitting when you type, so using a **firewall** is vital to filter out these kinds of programs.

Avatar: A graphical representation of a person. Avatars are sometimes used in chat and multi-user gaming environments.

Blog: A blog, also known as a weblog, is a form of online diary or journal. Blogs contain short, frequently updated posts, arranged chronologically with the most recently posted item appearing at the top of the page. In addition to text, blogs can contain photos, images, sound, archives and related links, and can incorporate comments from visitors.

Bluetooth: Bluetooth is a telecommunications industry standard which allows mobile phones, computers and PDAs to connect using a short-range wireless connection.

Bookmarking: The process of storing the address of a website or internet document on your computer, so that you can find it again easily.

Chatroom: An area on the internet or other computer network where users can communicate in real time, often about a specific topic. As chat software develops, individuals are not only able to send text messages to chat rooms but, in some instances, also have the ability to communicate through their actual voices (voice chat) via headsets, or indeed, actually be seen by chat room members, through web cams.

When joining a chat service or room an individual must select an onscreen name or nickname, and all members of a chat room are usually listed down one side of the screen. As well as chatting in a specific room, individuals can request and initiate private conversations with other members of a chat room, which can appear similar to instant messaging.

Cookie: a piece of data stored in your computer after you have visited a website, that allows the web page to be down loaded more quickly.

Cyberspace: *Cyberspace* is a metaphor for the environment in which communication over computer networks occurs. The word is often used as an alternative to *internet*.

Digital video: Video captured, manipulated and stored in a digital format.

Filtering: A method used to prevent or block users' access to unsuitable material on the internet.

Firewall: A network security system used to restrict external and internal traffic.

Hacking: The process of illegally breaking into someone else's computer system breaching the computer's security.

Internet service provider (ISP): A company providing a connection to the internet and other services, such as browser software, email, a helpline, web space and subscriber-only content.

Instant messaging (IM): Allows users to communicate with other users, providing an easy way of sending short written messages to a few friends online at the same time. It includes text messaging, voice chat, webcams, and file and picture exchange. IM can be a very private form of communication between known friends where the user builds up a list of contacts and is alerted when they are online. IM, however, can also be a public open environment where the user is encouraged to find and make new contacts online.

P2P (peer to peer): The internet is beginning to offer new services alongside websites and chat services, particularly those which enable the swapping and storing of media files (sounds, images and video). This is referred to as *Web 2.0*. These services can enable direct sharing of files – person to person, computer to computer. These services are much harder to moderate than chat rooms and message boards. As ISPs and service operators bring in moderation to make sure their digital services with a social function are safer for children, technology is encouraging social activity away from these safe centres. This means that educating children and young people how to protect themselves online becomes even more important.

Personal digital assistant (PDA): A small, mobile, handheld device that provides computing and information storage/retrieval capabilities, and possibly phone facilities too.

Phishing: When someone tricks you into giving confidential information by asking you to click on a false website and entering your details.

Spam: Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

SMS: Short messaging service or text messages.

Spoofing: Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan horses: A virus which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.

Usenet: The part of the internet where **newsgroups** are found.

Video conferencing: The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.

Vlog: A **blog** which showcases video.

Virus: A computer program which enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

WAP: A website designed to be accessed on a small screen like a mobile phone.

Webcam: A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.

Weblog: See the entry for 'blog' above.

WIFI: Short for wireless fidelity, it is a way of connecting a computer to the internet using radio frequency, rather than cables. A hotspot is where you can access a WIFI network.

Appendix 2 - Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of communications. Many people use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

"Organisations have a right (and in the case of providing services to children, a duty) to monitor use of their technical infrastructures to prevent them 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.

In any case, organisations should be open on the subject of monitoring the use of their technical networks, and this can typically be achieved through the acceptable use policy, as previously discussed." (BECTA)

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- Gain access to computer files or software without permission (for example using someone else's password to access files);
- Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- Impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

"The Regulation of Investigatory Powers Act (RIPA) provides 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.

Each police force and most councils are defined as a 'public authority' to which RIPA applies. 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 RIPA. No covert directed surveillance or use of covert human intelligence sources may be undertaken without obtaining authority from such an authorising officer.

RIPA requires that third parties that are required 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 RIPA. As such, they should be aware of the appropriate response if such a request is made." (Ref: BECTA 2007)

The Telecommunications (Lawful Business Practice) (Interception of Communications)

Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation. Internet use and abuse is governed by many civil or criminal laws in the UK. While this list is not exhaustive, some of the key provisions are summarised below:

- Computer Misuse Act 1990 (including hacking, denial of service attacks)
  http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

- Copyright, Designs and Patents Act 1988(including copyright theft)
  http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

- Crime and Disorder Act 1998
  http://www.opsi.gov.uk/acts/acts1998/19980037.htm

- Data Protection Act 1998
  http://www.opsi.gov.uk/acts/acts1998/19980029.htm

- Privacy and Electronic Communications (EC Directive) Regulations 2003(including spam)
  http://www.opsi.gov.uk/si/si2003/20032426.htm

- Protection from Harassment Act 1997 (including harassment, bullying, and cyber stalking)
  http://www.opsi.gov.uk/acts/acts1997/1997040.htm

- Protection of Children Act 1978, as amended by Section 84 of the Criminal Justice and Public Order Act 1994 (including indecent images of children)
  http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm

- Malicious Communications Act 1988 (including harassment, bullying, and cyber stalking)
  http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm

- Sexual Offences Act 2003 (including grooming)

http://www.opsi.gov.uk/acts/acts2003/20030042.htm

- The Obscene Publications Act 1959 and 1964 (including illegal material on, or transmitted via, the web and electronic communications) - not available online

- The Telecommunications Act 1984 (including illegal material on, or transmitted via, the web and electronic communications) - Not available online

Appendix 3 - Sources of external e-safety support

There are a number of agencies that can provide help either in terms 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 are described briefly below.

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

The Child Exploitation and Online Protection (CEOP) Centre aims to tackle child sex abuse wherever and whenever it happens. Part of their strategy for achieving this is to provide internet safety advice for parents and carers, training for educators and child protection professionals, and providing a 'virtual police station' for reporting abuse on the internet.

Some of these services are outlined briefly below.

Thinkuknow – online safety for young people and their parents
[http://www.thinkuknow.co.uk]

The CEOP Thinkuknow website provides 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 TV.

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

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

A section of the website is aimed specifically at parents and carers to try to help them understand more about what their child may be doing online.

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

Training for educators
[http://www.thinkuknow.co.uk/teachers]

CEOP offers training to educational professionals through the Thinkuknow Education Programme, aimed at children aged 11-16.

Once trained, educators are able to directly deliver the Thinkuknow programme to children. Further completion of the CEOP Ambassador Training scheme will also allow educators to cascade the training to colleagues. The authority has a trained CEOP Ambassador so if your schools would like some training, please contact Mark Churchill.

Training for child protection professionals
http://www.ceop.gov.uk/training/courses.html

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

They provide 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 better understand the nature of sexual offending and to develop the skills and knowledge that can better equip professionals to deal with the very 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, to report any inappropriate or potentially illegal activity towards a child online. 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 immediate 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.

Virtual Global Taskforce
http://www.virtualglobaltaskforce.com

The Virtual Global Taskforce (VGT) is made up of law enforcement agencies from around the world 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 provides links to a range of useful resources, and the site also provides a direct link for reporting abuse.

Internet Watch Foundation
http://www.iwf.org.uk

The Internet Watch Foundation (IWF) is the UK hotline for reporting illegal content, specifically child abuse images hosted worldwide and content that is criminally obscene and incitement to racial hatred, hosted in the UK. A prominent link for reporting illegal content is available from the homepage of the IWF website.

The IWF website also provides an overview of the IWF URL list of online child abuse content, which should be included as an absolute minimum in internet filtering services

NSPCC and related services
http://www.nspcc.org.uk

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 can call 0800 1111 to talk about any problem, 24 hours a day.

There4me.com

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

Child Protection Helpline

The NSPCC Child Protection Helpline offers advice and support to anyone 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! aims to prevent child sexual abuse by increasing public awareness and empowering people to act responsibly to protect children.

Stop it Now! operates a freephone helpline on 0808 1000 900. It offers confidential advice and support to adults that might be unsure or worried about their own thoughts or behaviour towards children, or the behaviour of someone they know, whether they are 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.

(Adapted from BECTA: safeguarding children in a digital world: Developing an LSCB e-safety strategy)

Bullying online
http://www.bullying.co.uk

Bullying Online is an online help and advice service combating all forms of bullying. Recognising that many young people that have lost friends through being bullied in the real world may turn to the internet to make new friends, the 'Staying safe in cyberspace'

section gives tips for staying safe in chat rooms. There is also a section on mobile phone bullying, giving tips on how to protect yourself, and information on how the law can help. The site provides information for pupils, teachers and parents.

Parentscentre
http://www.parentscentre.gov.uk

Parentscentre offers support, information and advice on children's learning and the education system, including use of the internet.

Safer working practices for adults working with technology with children and young people

Professionals (including volunteers) working with children and young people must appreciate the nature and responsibilities of their professional roles that places them in a position of trust with children and young people.
Guidance to safer working practices with technology aims to:
Ensure that children and young people are safeguarded in the digital world
Provide professionals with advice and good practice, and work towards a culture of vigilance in workplace.
Assist professionals to comply with their own Codes of Practices/ Acceptable Use of Internet policies
Minimise risks of allegations of abuse or inappropriate behaviours against staff members.
Project a clear message that unlawful or unsafe / risky behaviours with IDMT are unacceptable and disciplinary action will be taken in line with council policies.

Acknowledgments

This document draws upon existing good practice and guidance provided by:

BECTA (2007) Safeguarding children online: a check list for Local Authorities and Local Safeguarding Children Boards
BECTA (2008) Safeguarding Children in a digital world
Internet Abuse Guidelines 2010, Essex and London Safeguarding Children Boards
CEOP www.ceop.org.uk
Kent: e-safety policy www.clusterweb.org.uk
North Yorkshire e-safety policy
Lambeth e-safety policy