

Hampshire, Isle of Wight, Portsmouth & Southampton 4LSCB E-Safety Strategy

Produced May 2009
Revision Date September 2011



Hampshire
Safeguarding
Children
Board



Table of Contents

Introduction	3
Summary	3
E-Safety Risks & Issues	4
Content:	4
Contact:	4
Commerce:	4
Safeguarding Against E-Safety Risks & Issues	4
PIES Model for Limiting E-Safety Risks	5
Policies & Practice	5
Procedures	6
Infrastructure & Technology	7
Education & Training	7
Glossary of Related Terms, Information & Organisations	8
Contact Details	9

Introduction

The Hampshire, Isle of Wight, Portsmouth & Southampton 4LSCB* takes seriously the statutory role they have to ensure that member agencies co-operate to safeguard and promote the welfare of children and young people in Hampshire, Isle of Wight, Portsmouth & Southampton 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 4LSCB has developed this E-Safety strategy built on four key areas:

- Policies, practices and procedures
- Education and training
- Infrastructure and technology
- Standards and inspection.

The 4LSCB 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.

Summary

“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”

Becta 2008- Safeguarding Children in a Digital World

E-Safety is the process of limiting risks to children and young people when using Information and Communications Technology (ICT). E-Safety is primarily a safeguarding issue not a technological issue, which relates to the use of all ICT-fixed or mobile; current, emerging and future ICT.

ICT is used daily as a tool to improve teaching, learning, communication and working practices to the benefit of our children and young people and those that work to support them. The use of ICT is recognised as being of significant benefit to all members of our community, in personal, social, professional and educational contexts. However alongside these benefits are potential risks that we have a statutory duty of care to manage, to ensure they do not become actual dangers to children and young people in our care or for employees.

* www.4lscb.org.uk

E-Safety Risks & Issues

E-Safety risks and issues can be roughly classified into three areas: content, contact and commerce. The following are basic example of the types of e-safety risk and issues that could fall under each category.

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
- Downloading of copyrighted materials, e.g. music and films
- Plagiarism

Contact:

- Grooming using ICT, leading to sexual assault and/or child prostitution
- Bullies using ICT (email, mobile phones, chat rooms etc) as a way to torment their victims
- Children and young people self-publishing information-sometimes inappropriate- about themselves and therefore putting themselves at risk
- Parents or carers meeting people of concern via the internet

Commerce:

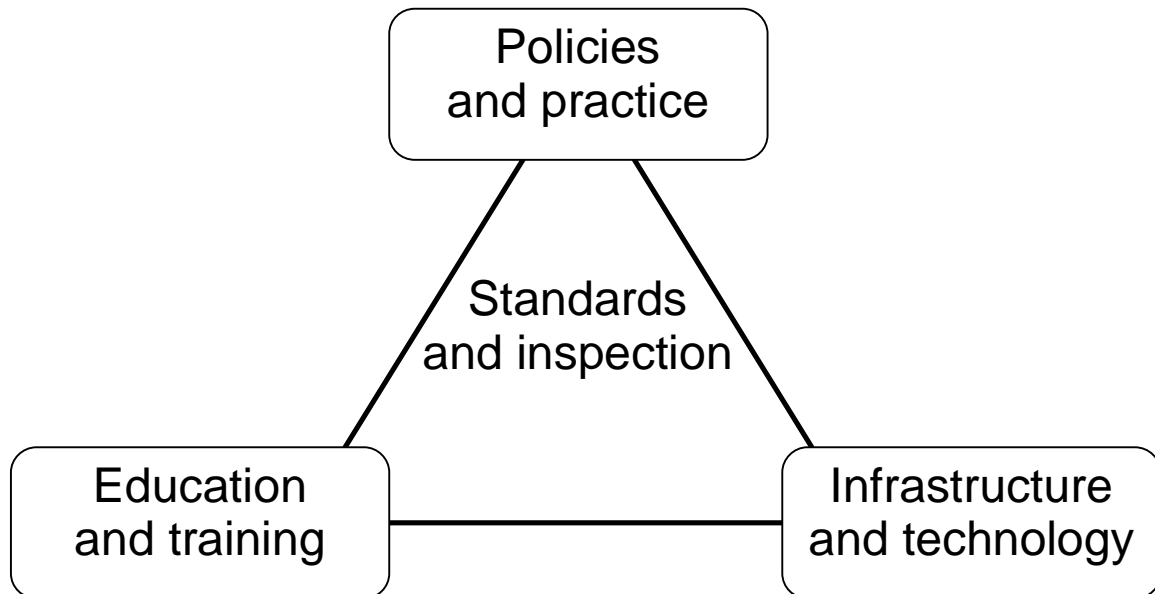
- Exposure to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Safeguarding Against E-Safety Risks & Issues

Stay safe is one of the aims of Every Child Matters. We all have a duty of care (albeit at different levels of responsibility) to safeguard and promote the welfare of children and young people, and as technology increasingly permeates into every aspect of our lives and from an ever younger age, we have a responsibility to deal with potential e-safety issues and to promote safe and responsible behaviour.

BECTA recommends a strategic approach to e-safety. This model illustrates how a combination of effective policies and practices, training and education, technology and infrastructure underpinned by standards and inspection can be an effective approach to manage and limit e-safety risks.

PIES Model for Limiting E-Safety Risks



Becta 2008 - Safeguarding Children in a Digital World

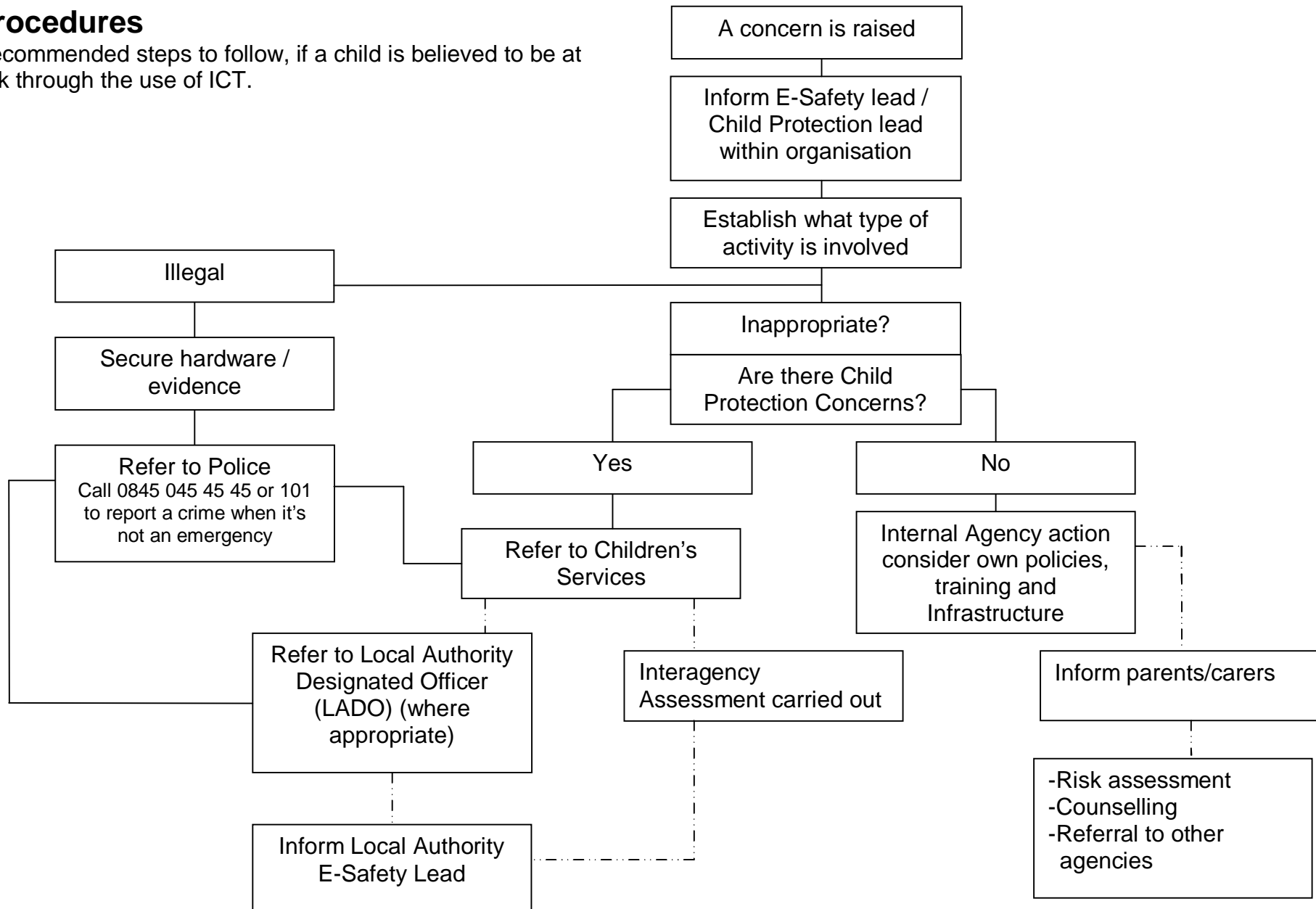
Policies & Practice

Any organisation that has contact with children and young people who may have access to ICT should have an e-safety policy which considers the following issues:

- The acceptable use of ICT by all users
- E-Safety procedures, e.g. incidents of misuse of ICT by users, safeguarding incident when a user is at risk or has come to actual harm through the use of ICT
- E-Safety training to be incorporated into the Children's Workforce Strategy (CWS), e.g. safety awareness, acceptable use, safeguarding procedures
- The technology and its security settings e.g. virus protections, filtering and monitoring.

Procedures

Recommended steps to follow, if a child is believed to be at risk through the use of ICT.



Infrastructure & Technology

All organisations providing services to children and young people which also provide access to ICT should consider the use of additional software and/or settings to limit the e-safety risk. Becta recommends that where Internet access is also available, it should be filtered and configured to the organisations own local circumstances and requirements; this product should meet or exceed the following requirements:

- Block 100% of illegal material identified by the Internet Watch Foundation (IWF) Child Abuse Images and Content (CAIC) URL List.
- Capable of blocking 90% 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 and software piracy

Education & Training

There are many training resources and support materials dealing with the issues of E-Safety with children, young people, parents and professionals which can be used by your organisation.

Professionals

Becta	http://www.becta.org.uk/safeguarding.php
Child Exploitation and Online Protection Centre (CEOP)	http://www.ceop.gov.uk/
Childnet International	http://www.childnet-int.org
Internet Proficiency Scheme	Scheme for Key Stage 2 pupils (DCSF, 2003)
Know IT All	http://www.childnet-int.org/kia/
Signposts to safety	http://www.becta.org.uk
Think U Know	http://www.thinkuknow.co.uk/

Children, Young People & Families

Kidsmart	http://www.kidsmart.org.uk/
Get Safe Online	http://www.getsafeonline.org/
Know IT All	http://www.childnet-int.org/kia/parents/
Parents Centre	http://www.parentscentre.gov.uk
Think U Know	http://www.thinkuknow.co.uk/

Glossary of Related Terms, Information & Organisations

Becta leads the national drive to inspire and lead the effective and innovative use of technology throughout learning. It's our ambition to create a more exciting, rewarding and successful experience for learners of all ages and abilities enabling them to achieve their potential.

<http://www.becta.org.uk>

Blogging & Social Networking is part of a social and technological revolution that some people are calling Web 2.0. What's different about it is the ease with which anyone can produce and distribute their own content and link with like minded sites to create a very powerful network for sharing ideas and influence opinion. Young people especially love this new environment because they can have a powerful voice to express their identity and opinions. However there are safety issues to consider for both young users, parents, industry and education.

<http://www.childnet-int.org/blogsafety/index.html>

CEOP - The Child Exploitation and Online Protection Centre is part of UK police and is dedicated to protecting children from sexual abuse wherever they may be. That means building intelligence around the risks, tracking and bringing offenders to account either directly or with local and international forces and working with children and parents to deliver our unique ThinkuKnow educational programme. Our approach is truly holistic, our style is totally inclusive and our appeal is to everyone out there to work with us in making every child matter, everywhere.

<http://www.ceop.gov.uk/>

Childnet International's mission is to work in partnership with others around the world to help make the Internet a great and safe place for children.

Childnet works in 3 main areas of Access, Awareness, Protection & Policy.

<http://www.childnet-int.org/>

CWS – Children's Workforce Strategy

Cyberbullying is the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else.

<http://www.digizen.org/cyberbullying/>

DCSF - The purpose of the Department for Children, Schools and Families is to make this the best place in the world for children and young people to grow up. We want to:

- make children and young people happy and healthy
- keep them safe and sound
- give them a top class education
- help them stay on track.

<http://www.dcsf.gov.uk/>

Downloading refers to receiving information or data electronically usually through the Internet; this could include saving a document or picture from a website or media streaming, e.g. music or video. Uploading is the inverse; sending and saving information or data from a local system e.g. mobile phone or computer, to a remote system, e.g. a website

E-Safety is the process of limiting risks to children and young people when using Information and Communications Technology (ICT). E-Safety is primarily a safeguarding issue not a technological issue, which relates to the use of all ICT-fixed or mobile; current, emerging and future ICT.

Every Child Matters: Change for Children is a new approach to the well-being of children and young people from birth to age 19.

The Government's aim is for every child, whatever their background or their circumstances, to have the support they need to:

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

<http://www.everychildmatters.gov.uk/>

Hacking is when your details, online accounts or other personal information is accessed by a stranger.

<http://www.ceop.gov.uk/reportabuse>

Filtering software can help to block a lot of inappropriate material but they are not 100% effective and are no substitute for good parental involvement. Internet use at school is generally filtered, supervised and safe. But many children use the Net at friend's homes, Internet cafes, libraries and youth clubs where there may be no filters and little supervision.

<http://www.childnet-int.org/>

A **Firewall** is a buffer between your computer and the Internet. It limits both incoming and outgoing information, and keeps your computer safe from intruders. It can't stop you downloading spyware, but it can alert you if a program is sending information over the Internet without your permission.

<http://www.childnet-int.org/sorted/>

Hampshire 4LSCB – Local Safeguarding Children Boards for Hampshire, Isle of Wight, Portsmouth and Southampton

ICT – Information and Communications Technology, e.g. mobile phones, gaming consoles, computers, email, social networking

Identity Theft is when your personal information is used by someone else without your knowledge. It may support criminal activity, which could involve fraud or deception [*The Home Office*]

<http://www.childnet-int.org/sorted/>

IWF – The Internet Watch Foundation was established in 1996 by the UK internet industry to provide the UK internet 'Hotline' for the public and IT professionals to report potentially illegal online content within our remit and to be the 'notice and take-down' body for this content. We work in partnership with the online industry, law enforcement, government, the education sector, charities, international partners and the public to minimise the availability of this content, specifically, child sexual abuse content hosted anywhere in the world and criminally obscene and incitement to racial hatred content hosted in the UK.

<http://wap.iwf.org.uk/>

Know IT All for Parents contains advice for parents and carers, and a special section for children and young people.

"I am delighted with this new resource. I have seen it myself and, as a new parent, I can see how valuable this will be to the parents of children and young people of all ages. We should never take for granted that our children know it all about computers and the internet. We should know what they're doing and be there to help and support them. This new resource provides a lot of information and advice for parents and I'm pleased that the main overview section is translated into seven other languages and into British Sign Language... I am also pleased that it includes sections for young people themselves and for teachers, and fully approve of the approach Childnet has taken with this resource – having young people talking to young people about the benefits and issues associated with the internet is very powerful." Parmjit Dhanda, MP, Minister for Children, Young People and Families speaking at the launch of the Know IT All for Parents resource

<http://www.childnet-int.org/kiia/parents/>

LADO - Local Area Designated Officer

LSCB - Children can only be safeguarded properly if the key agencies work effectively together. Local Safeguarding Children Boards (LSCBs) are designed to help ensure that this happens. The core membership of LSCBs is set out in the Children Act 2004, and includes local authorities, health bodies, the police and others. The objective of LSCBs is to coordinate and to ensure the effectiveness of their member agencies in safeguarding and promoting the welfare of children.

<http://www.everychildmatters.gov.uk/lscb/>

Report Abuse

<http://www.ceop.gov.uk/reportabuse>

Spam & Phishing "Spam: Commercial e-mails, generally advertising products or services available to buy online, sent to a large number of recipients without their consent. Phishing: Internet fraudsters who send spam or pop-up messages to lure personal information from unsuspecting victims." US Federal Trade Commission

<http://www.childnet-int.org/sorted/>

Spyware & Adware "A general term for malicious software that is designed to take control of a computer without the consent of the user. Adware is one type of spyware - computer programs in which commercial advertisements are automatically shown to the user without their consent." Wikipedia.org

<http://www.childnet-int.org/sorted/>

URL – Universal Resource Locator or website address

VOIP - Voice Over Internet Protocol

**Hampshire, Isle of Wight,
Portsmouth & Southampton 4LSCB**
E-Safety Strategy

Hampshire Safeguarding Children Board
Telephone 01962 876230
Email hscb@hants.gov.uk

Southampton Safeguarding Children Board
Telephone 023 8083 2995
Email natasha.newcombe@southampton.gov.uk

Portsmouth Safeguarding Children Board
Telephone 02392841540
Email sallie.ridgley@portsmouthcc.gov.uk

Isle of Wight Safeguarding Children Board
Telephone 01983 814545
Email rosie.rae@iow.gov.uk