LSCB

Bath & North East Somerset
Local Safeguarding Children Board

Bath and North East Somerset E-Safety Strategy

Date approved by LSCB Revision Date	December 2015 Revised June 2016 to update advice in Appendix A
Author	Original Author: Richard Baldwin Review Author: Richard Baldwin
Date for review	December 2018
Detail of review amendments	Updated to reflect the Serious Crime Act (2015) which introduced an offence of sexual communication with a child.

Contents

Amendment
In September 2015, this chapter was updated to reflect the Serious Crime Act (2015) which introduced an offence of sexual communication with a child. This applies to an adult who communicates with a child and the communication is sexual or if it is intended to elicit from the child a communication which is sexual and the adult reasonably believes the child to be under 16 years or age. The Act also amended the Sex Offenders Act 2003 so it is now an offence for an adult to arrange to meet with someone under 16 having communicated with them on just one occasion (previously it was on at least two occasions).

Introduction

Safeguarding is everyone's responsibility and the Local Safeguarding Children's Board in Bath and North East Somerset take 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 Bath and North East Somerset and to ensure that they are effective in doing so.

As part of safeguarding and promoting the welfare of children and young people in accordance with the Children Act 2004 and Working Together to Safeguard Children (HM Government, 2013), the LSCB 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 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.

Purpose of the Strategy

The LSCB is committed to raising awareness of e-safety issues to all partner organisations and promoting good practice to reduce risks to children and young people when they are online or when using digital electronic technologies.

This strategy has been written to provide the e-safety framework for member agencies of the LSCB and other agencies and organisations who work with children and young people within the Bath and North East Somerset area.

It cannot, and does not attempt to, cover all arrangements for agencies, organisations and educational establishments working in the area and should be seen as guidance to help inform what local agencies, organisations and educational establishments need to do to ensure they are equipped to safeguard and promote the welfare of children and young people in a digital age. The strategy recognises that being safe on line is not just a matter of technology and that a comprehensive approach to e- safety is necessary.

Note: The Serious Crime Act (2015) has introduced an offence of sexual communication with a child. This applies to an adult who communicates with a child and the communication is sexual or if it is intended to elicit from the child a communication which is sexual and the adult reasonably believes the child to be under 16 years or age. The Act also amended the Sex Offenders Act 2003 so it is now an offence for an adult to arrange to meet with someone under 16 having communicated with them on just one occasion (previously it was on at least two occasions).

Where there are concerns in relation to a child's exposure to extremist materials, the child's school may be able to provide advice and support; all schools are required to identify a Prevent Single Point of Contact (SPOC) who is the lead for safeguarding in relation to protecting individuals from radicalization and involvement in terrorism.

Suspected online terrorist materials can be reported through GOV.UK. Content of concern can also be reported directly to social media platforms – see UK Safer Internet Centre website.

Where there is concern that a member of staff or someone in a position of trust has acted inappropriately a referral to the LADO should be considered.

Background

> "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, there 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. Social networking sites are often used by perpetrators as an easy way to access children and young people for sexual abuse. In addition, radical and extremist groups may use social networking to attract children and young people into rigid and narrow ideologies that are intolerant of diversity: this is similar to the grooming process and exploits the same vulnerabilities. The groups concerned include those linked to extreme Islamist, or Far Right/Neo Nazi ideologies, Irish Republican and Loyalist paramilitary groups, extremist Animal Rights groups and others who justify political, sexist or racist violence.

What is E-Safety?

E-Safety is a term that encompasses not only the internet, but all other ways in which young people communicate using electronic media (eg; smart phone, gaming consoles). It means ensuring that young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves and others.

This guidance is designed to assist front-line practitioners to;

a) Guide young people and others to the best sources of information and support (not duplicate) the range of advice and resources already available.
b) Assist organisations to develop their own solutions and to incorporate the

principles and priorities in this strategy into those.

c) Identify those young people who are potentially vulnerable
d) Ensure that risk is assessed and managed effectively
e) Make sure that young people understand their own risks when using online services.

E-Safety Risks & Issues

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

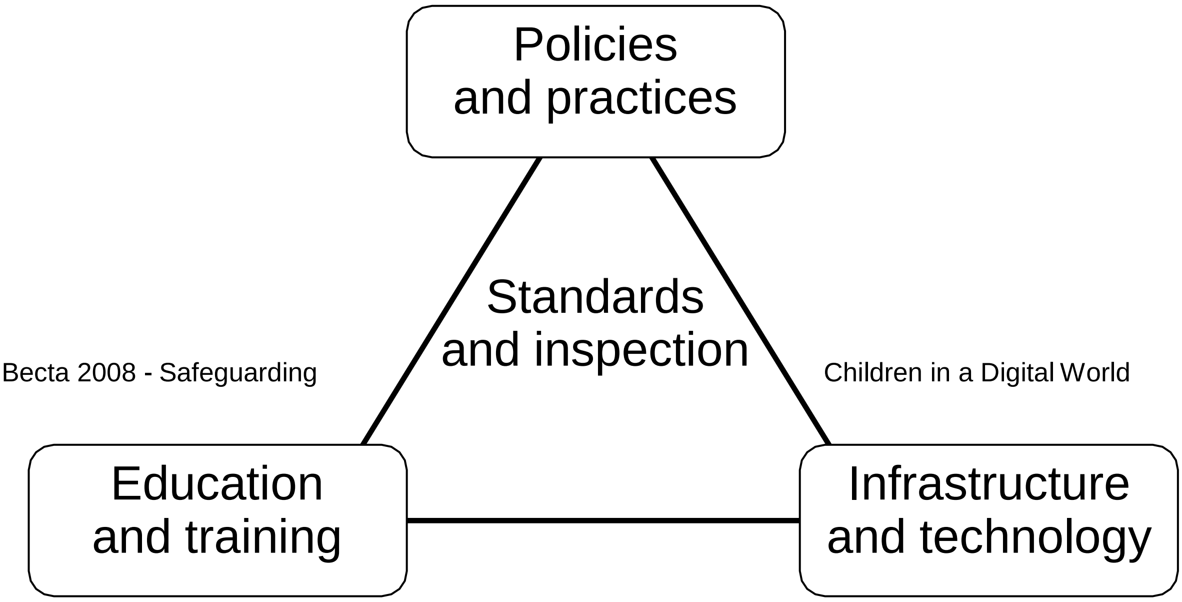
	Commercial	**Aggressive**	**Sexual**	**Values**
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting personal info	Being bullied, harassed 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

DSCF, 2008 - Safer Children in a Digital Word: The report of the Byron Review

Key Measures for Limiting E-Safety Risks

The LSCB supports the use of the Becta PIES model which offers an effective strategic framework for approaching e- safety. This model illustrates how a combination of effective policies and practices, education and training, infrastructure and technology 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 & Practices

Any organisation that has contact with children and young people should:

- Appoint a dedicated e-safety lead;
- Create and maintain an e-safety policy;
- Make sure that appropriate Acceptable Use of ICT Policy and Staff User Agreements are in place;
- Have a procedure in place for reporting an e-safety incident, e.g. clear lines of reporting incidents of misuse of ICT by users and safeguarding incidents when a user is at risk or has come to actual harm through the use of ICT;
- Review and evaluate all internal policies and procedures (at least every 12 months or in response to new technologies or e-safety incidents if sooner.

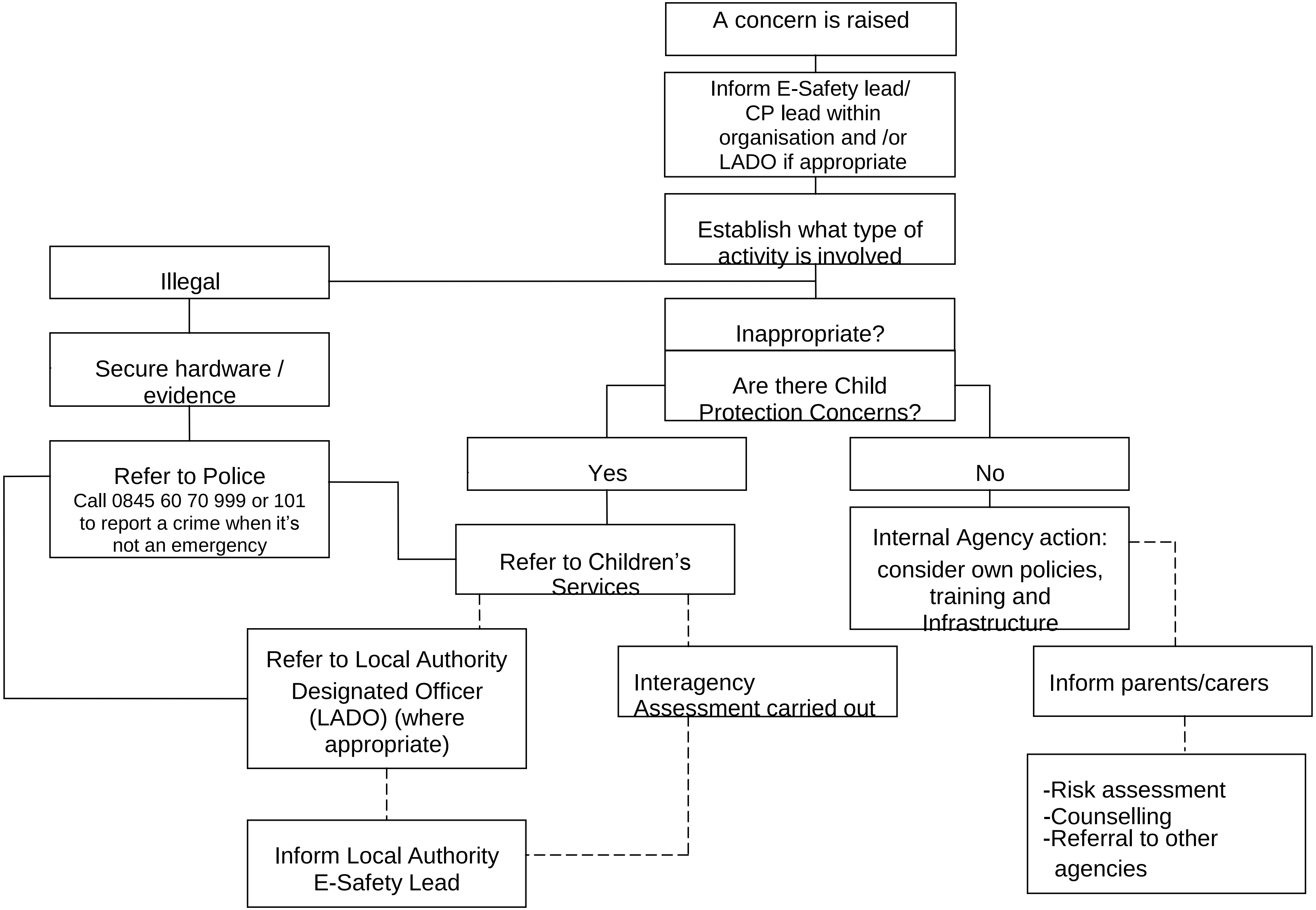
Schools and other young people's organisations are encouraged and supported to ensure that e-safety is at the heart of their efforts to safeguard young people. This should be as part of the PSHE curriculum and other pastoral care.

BANES LSCB supports the Zip-it, Block it, Flag it safety code. This code features three simple and memorable actions to remember.

a) Zip it; Means keeping personal stuff private and thinking about what you do online
b) Block it; reminds you to block people who send nasty messages and not to open any links and attachments which are received by e-mail or through social networks
c) Flag it; This stands for flagging up to a parent, teacher or guardian, or someone in authority anything that upsets them while they are online, or if someone asks to meet them in the real world.

Procedures

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



A concern is raised
Inform E-Safety lead/ CP lead within organisation and /or LADO if appropriate
Establish what type of activity is involved
Illegal
Secure hardware / evidence
Refer to Police
Call 0845 60 70 999 or 101 to report a crime when it's not an emergency
Inappropriate?
Are there Child Protection Concerns?
Yes
No
Refer to Children's Services
Internal Agency action: consider own policies, training and Infrastructure
Refer to Local Authority Designated Officer (LADO) (where appropriate)
Interagency Assessment carried out
Inform parents/carers
Inform Local Authority E-Safety Lead
-Risk assessment
-Counselling
-Referral to other agencies

Infrastructure & Technology

All organisations providing services to children and young people which also provide access to ICT should:

- Identify all technologies used within the organisation itself and carry out risk assessments with regards to e-safety;
- Consider the use of additional software and/or settings for technologies to limit the e-safety risk;
- Use up to date security software / solutions for technologies;
- Where Internet access is available, Becta advises that a web content filtering product or service must as a minimum:

i) Subscribe to the Internet Watch Foundation Child Abuse Images and Content (CAIC) URL List;

ii) Block 100% of illegal material identified by the Internet Watch Foundation (IWF);

iii) 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

Any organisation that has contact with children and young people should aim to raise awareness of e-safety through education and training.

E-safety training should be incorporated into the organisation's children's workforce training strategy, e.g. safety awareness, acceptable use, safeguarding procedures. This should include induction of new staff, plus on-going support and supervision of existing staff. Staff should be made aware of local, regional and national issues with regards to e-safety and should be confident in their abilities to escalate an incident as necessary and appropriate.

An organisation should also consider their role in giving e-safety information and guidance to children, young people, parents and carers.

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

CEOP (Child Exploitation and Online Protection) Safety Centre	http://www.ceop.police.uk/safety-centre
Childnet International	http://www.childnet.com
Know IT All	http://www.childnet-int.org/kia/
Professionals Online Safety Helpline (UKSIC)	Email helpline@saferinternet.org.uk or telephone 0844 381 4772
SWGfL Staying-Safe (South West Grid for Learning)	http://www.swgfl.org.uk/Staying-Safe
Think U Know (CEOP)	http://www.thinkuknow.co.uk/
UK Safer Internet Centre (UKSIC)	http://www.saferinternet.org.uk/
Helping parents keep their children safe online	www.internetmatters.org

Children, Young People & Families

A Parent's Guide to Technology (UKSIC)	http://www.saferinternet.org.uk/advice- and-resources/a-parents-guide
Connect Safely	http://www.connectsafely.org
Digizen	http://www.digizen.org
KidSmart	http://www.kidsmart.org.uk/
Get Safe Online	http://www.getsafeonline.org/
Know IT All	http://www.childnet-int.org/kia/parents/
Think U Know	http://www.thinkuknow.co.uk/
Helping parents keep their children safe online	www.internetmatters.org

Standards and Inspection

Quality assurance activity is essential to ensuring that policies and strategies are effective. This may include:

- Gathering relevant information to establish the extent of current awareness and training resources available;
- Review and evaluate all internal policies and procedures (at least every 12 months or in response to new technologies or e-safety incidents if sooner);
- Developing a mechanism for reporting the number of e-safety incidents;
- Developing an audit plan to assess the extent to which e-safety is incorporated into safeguarding activity.

Monitoring and Review of this Strategy

This strategy will be monitored and reviewed on an annual basis (or sooner in response to new technologies or e-safety incidents).

Glossary of Related Terms

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.com/blogsafety/index.html

Cyber bullying 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

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

http://www.childnet.com/downloading

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.

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 friends' homes, Internet cafes, libraries and youth clubs where there may be no filters and little supervision.

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.

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

http://www.ceop.police.uk/safety-centre

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.com/sorted

LADO - Local Area Designated Officer**.** The LADO is appointed by the local authority to manage allegations against people who work with children and young people.

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.

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.com/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.com/sorted

URL – Universal Resource Locator or website address

VoIP - Voice Over Internet Protocol “commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as Internet”. [Wikipedia.org]

Information & Organisations

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 Think U Know educational programme. http://ceop.police.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.com

DfE - The Department for Education is responsible for education and children's services.
http://www.education.gov.uk

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 their remit and to be the 'notice and take-down' body for this content. IWF works 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://www.iwf.org.uk

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

http://www.childnet.com/kia/parents/

Local Safeguarding Children Board

http://www.bathnes.gov.uk/services/children-young-people-and-families/child-protection/local-safeguarding-children-board

Report Abuse

http://ceop.police.uk/safety-centre

UK Safer Internet Centre (UKSIC) - The UK Safer Internet Centre is co-funded by the European Commission and brought to you by a partnership of three leading organisations, Childnet International, the South West Grid for Learning and the Internet Watch Foundation. The UK Safer Internet Centre has three main functions: An Awareness Centre, a Helpline and a Hotline.

http://www.saferinternet.org.uk

Appendix A

Advice for parents

Teaching your children how to use the internet safely is just as important as teaching them how to cross the road using the Green Cross rules. The following is designed for both parents and children with useful advice for each. So when your youngsters are online, whether alone or with you by their side, it's also as crucial to explain to them why they should remember these three simple and memorable actions. Here are some of the key bits to remember:

1. ZIP IT means keeping their personal stuff private and thinking about what they say or do online.

- People may not be who they say they are online so ensure children realise that adults do pretend to be children in chat rooms and on instant messaging systems.
- Set privacy controls to restrict access by strangers to your child's social network account. Remember, they should not be on Facebook unless they are over 13.
- Be aware that even the smallest piece of personal information placed online could be used to identify them.

2. BLOCK IT reminds them to block people who send them nasty messages and not to open any links and attachments they receive by email or through social networks if they're not 100 per cent sure they're safe.

- Use filters, parental controls and security settings on mobile phones and games consoles as well as on your computer.
- Set preferences on search engines to prevent them looking for inappropriate material. This can block the use of certain keywords.
- Sit with your child and make sure they know how to delete emails, or remove people from instant messengers.

3. FLAG IT is the final piece of advice. It stands for flagging up to a parent, guardian, teacher or someone in authority anything that upsets them while they are online or if someone asks them to meet up in the real world.

- Encourage your children to talk to a trusted adult if they don't feel they want to discuss a problem encountered online with you.
- Remind them never to meet anyone in the offline world that they have met online without you going with them.
- Make them aware of the Click CEOP buttons placed on the likes of Facebook and Windows Live Messenger. This allows them to report inappropriate sexual behaviour towards them directly to the authorities.

Following these three simple statements will not only keep your child safe, it will also help ensure your computer is safe from viruses, spam and malware that could steal your identity, money from your bank account or delete precious photos and videos stored on your hard drive.

Three quarters of young people say they couldn't live without the internet with a quarter admitting it would be the first place they turn for advice on alcohol, drugs, sex, finance and health.

Those findings by YouthNet prove just how the web is an increasing daily part of a young person's life.

But with nearly a fifth of those youngsters who have accessed the internet coming across something harmful or inappropriate (Staying Safe Survey, 2009) the need for a simple set of actions is obvious.

Information for young people

The internet is a great way to see more, learn more and have lots of fun. To help you enjoy it safely, you should follow these three simple things to remember that can help keep you safe when you visit your favourite websites.

Protect your own safety

The following is a list of three simple things to remember when you're online:

Zip it:

When you're online, always keep your personal stuff private and think about what you say and do.

Remember that people online may not be who they say they are. Online friends are still strangers, even if you have been talking to them for a long time.

Don't share personal information online. This includes:

- your full name
- photos
- addresses
- school information
- telephone numbers
- places you like to spend time

Make sure you have set your privacy settings to restrict access to personal information. When you use chat rooms or instant messenger, use a nickname instead of your real name. To stop people accessing your online accounts, always keep your passwords secret and change them regularly.

Block it:

Think about blocking people who send you nasty messages, and don't open unknown links and attachments.

Always delete emails from people you don't know, and don't open attachments from people you don't know. They might be nasty or contain a virus that can stop your computer working. If someone is mean or sends nasty messages online, block them.

Flag it:

If you see that anything upsets online or if someone asks to meet up with you, flag it up with someone you trust. If you are worried or unhappy about anything you see online, tell a parent or an adult you trust and they can help you. If you want to talk to someone else, you can call ChildLine 0800 1111.

If a friend you have made online asks to meet you in the offline world, talk to your parents or a trusted adult about it. You should never meet up with someone you have met online without an adult going with you because it is dangerous.

If someone you know is being nasty to someone online, speak to a parent or trusted adult about it.

Advice Amended June 2016