Buckinghamshire Safeguarding Children Board
BSCB Strategy: e-Safety
January 2014

Version Control			
Version number	**Date**	**Author**	**Comments and nature of update**
V2.0	January 2014		Revised by Policies and Procedures Sub Group

Introduction

The Buckinghamshire Safeguarding Children Board recognises the importance of e-safety in the context of Every Child Matters and its duty to safeguard and promote the welfare of children and young people. As technology and the internet play an increasing part in every aspect of a child's life, e-safety becomes a necessary part of this remit.

There is a wealth of existing information and resources available on e-safety. The BSCB e-Safety sub-committee policy is to draw on the best available information and resources and integrate this into existing BSCB safeguarding protection policies, safe working practice and local anti-bullying strategies.

This strategy aims to provide best practice and signpost readers to relevant information as well as incorporating the required referral process(es) which **must** be followed in the event of child protection concerns (Appendix one).

BSCB e-safety strategy

The BSCB e-safety strategy is to help achieve the aims set out by the UK Council for Child Internet Safety (UKCCISS).

These are:

- Creating a safer on line environment
- Giving everybody the skills, knowledge and understanding to help children and young people stay safe on line
- Inspiring safe and responsible use and behaviour

What this means for Buckinghamshire:

For Children & Young people:

- Understanding the risks of what they might find on line (accessing harmful and inappropriate content on the internet and video via games)

- Understanding the risks and consequences of their own and other people's online behaviour (people not being who they say they are, the dangers of on line actions and unsafe meeting arrangements)

- Offering clear guidance and advice about lawful, safe and responsible on line activity. This includes the taking, downloading and sharing of personal data and images, posting malicious and illegal content, and offensive behaviour such as bullying and racism

- What steps to take if they have concerns, including where to go for help and how to report abuse

For Adults:

- Understanding the risks associated with technology including social media, gaming and accessing the internet through computers and mobile devices

- Offering up to date information, clear guidance and advice about lawful, safe and responsible practice for adults to follow (for parents/carers and for those working in the children's workforce)

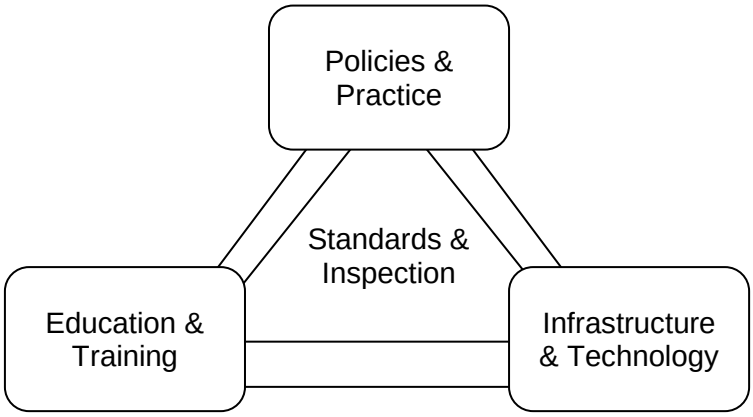
- Understanding what controls (including software) can be used to help keep children and young people safe

- Helping adults to equip children with the awareness, judgement and critical thinking skills to harness the huge benefits of the internet, whilst reducing their potential vulnerability to the risks

BSCB e-safety workplan

The BSCB e-safety sub committee has a work plan in place to help achieve the e-safety strategy. This is subject to regular review and monitoring at meetings of the e-safety sub-committee. The work of the e-safety sub committee is also reported on and scrutinised at meetings of the BSCB.

Our approach is to use the framework set out by BECTA in its publication 'Safeguarding Children in a Digital World', which looks at Policies, Infrastructure, Education and Standards (PIES). This helps agencies, organisations and/or service providers consider and manage the risks attached to e-safety.



The BSCB e-safety objectives are to *work towards* the following:

Policies & Practices

- Ensuring that e-safety is included in safeguarding policies, safe working practice procedures and anti-bullying procedures
- Ensuring there is an acceptable use policy for internet use and online activity in agency and/or service provider settings and that sanctions for breaches in behaviour are set out
- Ensuring that it is clear on how to report concerns
- Ensuring that resource and information are tailored to the needs of individual settings and are accessible, in particular, to the most vulnerable groups
- Ensuring that all aspects of the BSCB e-safety work plan are responsive to relevant developments and research

Infrastructure

- Ensuring that agencies and/or service providers have networks that are safe and secure
- Ensure that agencies and/or service providers use acceptable internet service providers
- Ensuring that filtering/monitoring products are in place

Education & training

- Ensuring that all users understand e-safety issues and how to manage risks including:
    - what safe and responsible on line behaviour means
    - on individual roles and responsibilities
    - on how to access/provide appropriate training and updates
    - on how to keep data safe and secure
    - on how to report concerns

Standards and Inspection

- Ensuring that agencies and/or service providers conduct an audit of e-safety measures by monitoring, reviewing and evaluating all of the above

Evaluating e-safety risks

E-safety risks can be classified around content, contact and conduct. The risks are often determined by behaviours relating to e-safety rather than the technologies themselves.

When on line for example, children may be exposed to inappropriate content. Some people may also use the internet to make contact with children and to groom them with the ultimate aim to exploit them sexually. ICT can also present opportunities for children and young people themselves to take part in inappropriate conduct by providing new channels for bullying behaviour, for example, through the use of hurtful text messages, videos or websites.

It is recognised that empowering measures that seek to teach children and young people to protect themselves online is more likely to be successful than a locked down response to technology which may deny learning opportunities.

	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, jacking, gambling, financial scams, terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

Table developed by the EUKids Online project as and referenced in paragraph 1.3 of the Byron Review, Safer Children in a Digital World, 2008.

Appendix 1

Referral process for e-safety concerns

- **Low level bullying**: the lead person for anti-bullying within organisation. Follow organisation's anti-bullying policy and procedures or seek advice from Bucks anti-bullying strategic lead - see http://www.buckscc.gov.uk/bcc/schools/bullying.page
- **Significant harm to a child/young person**: consult designated person for child protection within organisation. Follow organisation's safeguarding procedures regarding consultation/referral to Social Care – see www.bucks-lscb.org.uk
- **Allegations against a member of staff or a volunteer**: Follow organisation's procedures for allegations management regarding consultation process with designated senior manager for allegations and referral to the Local Authority Designated Officer – see www.bucks-lscb.org.uk
- **Emergency situations**: (where immediate significant harm to a child is occurring or anticipated) - contact the Police directly and without delay
- **Criminal activity**: (for example child pornography, extreme violence or extremist behaviour) – report to the Police without delay

Appendix 2

E-safety checklist

The following table will help agencies/service providers to monitor and evaluate their existing procedures and identify any gaps in adopting the BSCB e-safety strategy.

Does your setting		Do your staff		Do your users	
Have a safeguarding policy which makes reference to e-safety?	☐	Understand e-safety issues and risks?	☐	Understand e-safety issues and how to manage these risks?	☐
Have in place an acceptable use / e-safety policy?	☐	Know how to report and manage issues of concern	☐	Understand their roles and take responsibility for their own online behaviour	☐
Raise awareness on the key e-safety issues?	☐	Know how to keep personal data safe and secure?	☐	Respect the feelings, rights, values and intellectual property of others online	☐
Keep a log of e safety incidents which includes the outcomes and follow up actions?	☐	Know how to protect and conduct themselves professionally on line?	☐	Know who to go to for help and how to report an e-safety concern?	☐
Have a network which is safe and secure?	☐	Model good practice in the use of mobile phones and the internet when working with children and young people?	☐	Contribute to the development of e-safety policies and good practice?	☐
Use an accredited internet service provider?	☐	Liaise with parents and carers to keep them informed?	☐		
Use appropriate filtering and monitoring products?	☐				

Appendix 3

Some useful links

There are many useful sites for information. These are a few of them:

The UK Council for Child Internet Safety (UKCCIS)

This brings together organisations from industry, charities and the public sector to work with the Government to deliver the recommendations from Dr Tanya Byron's report – Safer Children in a Digital World

https://www.gov.uk/government/policy-advisory-groups/uk-council-for-child-internet-safety-ukccis

(CEOP) The Child Exploitation and Online Protection Centre

A multi-agency service dedicated to tackling the exploitation of children.
http://www.ceop.police.uk

Thinkuknow

CEOP's educational portal which has information and resources for children and young people, parents / carers, and professionals - covering all aspects of e-safety and new technology including mobiles. It also contains resources for qualified trainers and, most importantly, there's also a place which anyone can use to report if they feel uncomfortable or worried about someone they meet online.
http://www.thinkuknow.co.uk/

Childnet International

A non-profit organisation working with others to "help make the Internet a great and safe place for children" http://www.childnet-int.org/

Know IT All

A suite of education resources from Childnet designed to help educate parents, teachers and young people about safe and positive use of the internet. http://www.childnet-int.org/kia/

Insafe

A European network of Awareness centres promoting safe, responsible use of internet and mobile devices to young people. http://www.saferinternet.org/web/guest/home of which CEOP is a member