

# Safeguarding children online

## Are you managing online risks well?

“The schools visited needed to focus more consistently on a number of important areas. These included: developing a curriculum for e-safety which builds on what pupils have learnt before and which reflects their age and stage of development; providing training which enables all staff, not just teachers, to support pupils; and helping families to keep their children safe.”

Ofsted, February 2010 – *The safe use of new technologies*  
[www.ofsted.gov.uk/publications/090231](http://www.ofsted.gov.uk/publications/090231)



## What is the issue?

Schools have the opportunity to transform education and help pupils fulfil their potential and raise standards with ICT. But it's also important that pupils learn how to be safe when they are using these new technologies, particularly Web 2.0 collaborative technologies such as social networking sites, which are becoming an essential aspect of productive and creative social learning.

Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach. Indeed, Ofsted stated that schools need to "manage the transition from locked down systems to more managed systems to help pupils understand how to manage risk."

Children will experiment online, and while their confidence and enthusiasm for using new technologies may be high, their understanding of the opportunities and risks may be low, as will their ability for responding to any issues they encounter. Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks, wherever and whenever they go online; to promote safe and responsible behaviours in using technology both at school and in the home and beyond.

E-safety is more about behaviour than technology.

## Why do I need to take action?

- Schools have a duty of care and must ensure they are able to safeguard children, young people and staff.

In most cases, the misuse of ICT is not serious and can be dealt with at classroom level. In rare cases children can be in serious danger. Staff are also susceptible to risks, as is the integrity of the whole school community. The Ofsted evaluation schedule from Sept 2009 includes:

### Inspectors should evaluate:

- *how safe pupils feel in school, including their understanding of issues relating to safety, such as bullying.*
- *the extent to which the pupils feel able to seek support from the school should they feel unsafe.*
- *the effectiveness of the school's arrangements, including links with key agencies, for ensuring the safety of its pupils.*

### Inspectors should take into account:

- *the extent to which pupils are able to understand, assess and respond to risks, for example those associated with new technology.*
- *the extent to which the school helps pupils to keep themselves safe, including encouraging pupils to adopt safe and responsible practices and deal sensibly with risk, for example, using the internet.*

## What risks should we be guarding against?

The Byron Review has classified the risks as relating to **content**, **contact** and **conduct**.

The risk is often determined by **behaviours** rather than the technologies themselves.

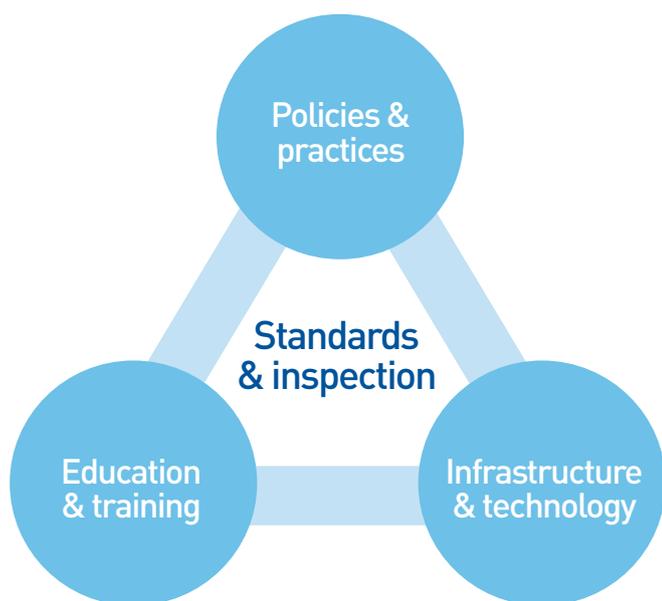
	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts, spam, sponsorship, personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias, racist, misleading info or advice
Contact (child as participant)	Tracking harvesting personal info	Being bullied, harassed 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

(Table developed by the EUKids Online project as and referenced in paragraph 1.3 of the Byron Review.)

Cyberbullying may be the biggest issue for your school but it's easier for adults to collect evidence about the bullying, from texts, e-mails or from monitoring software. It's important that all relevant policies (e.g. behaviour, bullying) include reference to cyberbullying.

# What should your school be doing?

Becta and other partner bodies have been developing advice and guidance on the issue of e-safety since 2000. Working with schools, teachers, young people, local authorities and Government, we have developed a model of support that can help to manage the level of risk. We believe that if you have the following PIES structure in place the e-safety risk can be effectively managed.



## Policies and practice

- Does the school have a set of robust policies and practices?
- Do you have an acceptable use policy (AUP)? Is everyone aware of it?
- Does your anti-bullying policy include references to cyberbullying?
- Are there effective sanctions for breaching the policy in place?
- Have you appointed an e-safety co-ordinator?

## Infrastructure

- Is the school network safe and secure?
- Do you use an accredited internet service provider?
- Do you use a filtering/monitoring product?

## Education and training

- Do all children receive e-safety education and training – where, how? Does this take into account prior learning and is it embedded throughout the curriculum?
- Are all staff – including support staff, and governors trained?
- Do you have a single point of contact in the school?
- Do the leadership team and school governors have adequate awareness of the issue of e-safety?

## Standards and inspection

- Have you conducted an audit of your school's e-safety measures?
- Do you monitor, review and evaluate all of the above?

# What does acceptable use look like in your school?

Have you got a robust acceptable use policy?

## Does it...

- reflect your setting and cover all users?
- have end-user input?
- promote positive uses of new and emerging technologies?
- clearly outline what network monitoring will take place?
- clearly outline acceptable and unacceptable behaviours when using technology and network resources provided by the school both on or offsite, or when using personal technologies on school premises or networks?
- clearly outline the sanctions for unacceptable use?

## Is it...

- clear and concise?
- written in a tone and style that is appropriate to the end-user?
- regularly reviewed and updated?
- widely, and regularly, communicated to all stakeholder groups?

## Where can I find good examples?

Look to your local authority and/or Regional Broadband Consortium for local policies.

In association with



© Copyright Becta 2010

You may reproduce this material, free of charge, in any format or medium without specific permission, provided you are not reproducing it for financial or material gain. You must reproduce the material accurately and not use it in a misleading context. If you are republishing the material or issuing it to others, you must acknowledge its source, copyright status and date of publication. While great care has been taken to ensure that the information in this publication is accurate at the time of publication, we accept no responsibility for any errors or omissions. Where a specific product is referred to in this publication, no recommendation or endorsement of that product by Becta is intended, nor should it be inferred.

**Becta** leading next generation learning

Millburn Hill Road  
Science Park  
Coventry CV4 7JJ

Tel: 0800 877 8777  
Fax: 024 7641 1418  
Email: [customerservices@becta.org.uk](mailto:customerservices@becta.org.uk)  
[www.becta.org.uk](http://www.becta.org.uk)

## Does your school...

- have a nominated e-safety co-ordinator?  
[www.becta.org.uk/safeguarding/esafetycoordinator](http://www.becta.org.uk/safeguarding/esafetycoordinator)
- audit its e-safety measures?  
<https://selfreview.becta.org.uk>  
[www.360safe.org.uk](http://www.360safe.org.uk)  
[www.nen.gov.uk/esafety](http://www.nen.gov.uk/esafety)
- have appropriate and robust acceptable use policies?  
[www.becta.org.uk/safeguarding/aups](http://www.becta.org.uk/safeguarding/aups)
- use a Becta accredited supplier for internet services?  
[www.becta.org.uk/safeguarding/accreditedsuppliers](http://www.becta.org.uk/safeguarding/accreditedsuppliers)
- include e-safety as part of your inspection evidence?  
[www.becta.org.uk/safeguarding/inspections](http://www.becta.org.uk/safeguarding/inspections)
- keep a log of e-safety incidents, resulting outcomes and follow-up actions?  
[www.becta.org.uk/safeguarding/loggingandmonitoring](http://www.becta.org.uk/safeguarding/loggingandmonitoring)
- handle cyberbullying issues well?  
[www.digizen.org/cyberbullying](http://www.digizen.org/cyberbullying)  
[www.teachernet.gov.uk](http://www.teachernet.gov.uk)
- raise awareness of e-safety issues by holding workshops and events?  
[www.becta.org.uk/safeguarding/raisingawareness](http://www.becta.org.uk/safeguarding/raisingawareness)  
[www.thinkuknow.co.uk/teachers](http://www.thinkuknow.co.uk/teachers)

## Do all your learners...

- understand what safe and responsible online behaviour means?  
[www.becta.org.uk/safeguarding/behaviour](http://www.becta.org.uk/safeguarding/behaviour)
- learn about e-safety in a range of subjects appropriate to their age and experience?  
[www.becta.org.uk/safeguarding/educatingchildrenandyoungpeople](http://www.becta.org.uk/safeguarding/educatingchildrenandyoungpeople)  
[www.becta.org.uk/safeguarding/smartrules](http://www.becta.org.uk/safeguarding/smartrules)  
[www.kidsmart.org.uk](http://www.kidsmart.org.uk)
- practice digital literacy skills, for example how to search safely and effectively online?  
[www.becta.org.uk/safeguarding/digitalliteracyskills](http://www.becta.org.uk/safeguarding/digitalliteracyskills)
- get the opportunity to share their views about staying safe online?  
[www.becta.org.uk/safeguarding/involvingchildrenandyoungpeople](http://www.becta.org.uk/safeguarding/involvingchildrenandyoungpeople)
- know how to report any concerns they may have?  
[www.ceop.police.uk/reportabuse](http://www.ceop.police.uk/reportabuse)

## Do all your staff and governors...

- understand e-safety issues and risks?  
[www.becta.org.uk/safeguarding/raisingstaffawareness](http://www.becta.org.uk/safeguarding/raisingstaffawareness)  
[www.nga.org.uk/uploadfiles/documents/NGA-Becta%20Sept.pdf](http://www.nga.org.uk/uploadfiles/documents/NGA-Becta%20Sept.pdf)
- receive regular training and updates?  
[www.becta.org.uk/safeguarding/educatingstaffandhelpers](http://www.becta.org.uk/safeguarding/educatingstaffandhelpers)  
[www.becta.org.uk/schools/communities/safetynet](http://www.becta.org.uk/schools/communities/safetynet)  
[www.childnet.com/kia](http://www.childnet.com/kia)  
[www.thinkuknow.co.uk/teachers](http://www.thinkuknow.co.uk/teachers)
- know how to support children and young people with new technologies?  
[www.becta.org.uk/safeguarding/supportingchildrenandyoungpeople](http://www.becta.org.uk/safeguarding/supportingchildrenandyoungpeople)  
[www.teachtoday.eu](http://www.teachtoday.eu)
- know how to report and manage issues or concerns?  
[www.becta.org.uk/safeguarding/reporting](http://www.becta.org.uk/safeguarding/reporting)  
[www.teachtoday.eu](http://www.teachtoday.eu)
- know how to keep data safe and secure?  
[www.becta.org.uk/safeguarding/datasafetyandsecurity](http://www.becta.org.uk/safeguarding/datasafetyandsecurity)
- know how to protect and conduct themselves professionally online?  
[www.becta.org.uk/safeguarding/professionalconduct](http://www.becta.org.uk/safeguarding/professionalconduct)  
[www.teachernet.gov.uk](http://www.teachernet.gov.uk)  
[www.teachtoday.eu](http://www.teachtoday.eu)
- take the opportunity to consult with children and young people in their care?  
[www.becta.org.uk/safeguarding/partnership](http://www.becta.org.uk/safeguarding/partnership)
- know about the updated e-safety guidance for QTS standard Q21a: Health and well-being?  
[www.tda.gov.uk/partners/ittstandards/guidance\\_08/qts/Q21a.aspx](http://www.tda.gov.uk/partners/ittstandards/guidance_08/qts/Q21a.aspx)

## Do all your parents and carers...

- understand e-safety issues and how to manage risks?  
[www.becta.org.uk/safeguarding/raisingparentalawareness](http://www.becta.org.uk/safeguarding/raisingparentalawareness)
- understand their roles and responsibilities?  
[www.becta.org.uk/safeguarding/roleofparentsandcarers](http://www.becta.org.uk/safeguarding/roleofparentsandcarers)
- receive regular training and updates?  
[www.becta.org.uk/safeguarding/educatingparentsandcarers](http://www.becta.org.uk/safeguarding/educatingparentsandcarers)  
[www.childnet.com/kia/parents](http://www.childnet.com/kia/parents)  
[www.thinkuknow.co.uk/parents](http://www.thinkuknow.co.uk/parents)
- understand how to protect their children in the home  
[www.nextgenerationlearning.org.uk/At-Home/Internet-safety](http://www.nextgenerationlearning.org.uk/At-Home/Internet-safety)

Need more help?

Our school e-safety co-ordinator is: