Schools

February 2009

Becta leading next generation learning

Safeguarding children online

How e-safe are your school and your learners?

"Children and young people need to be empowered to keep themselves safe – this isn't just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim."

Dr Tanya Byron
Safer children in a digital world: The report of the Byron Review

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. 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.

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 self-evaluation form (SEF) includes a new prompt specifically relating to e-safety.

  Question 4b reads: *To what extent do learners feel safe and adopt safe practices?*

  For example: *the extent to which learners adopt safe and responsible practices, dealing sensibly with risk, in a range of activities within and outside the classroom, including the use of new technologies and the internet.*

- The Byron Review has called on Ofsted to take various steps to hold schools to account for their performance in e-safety. All schools will need to actively monitor the impact of their e-safety policies and provide a comprehensive response to the SEF.

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.

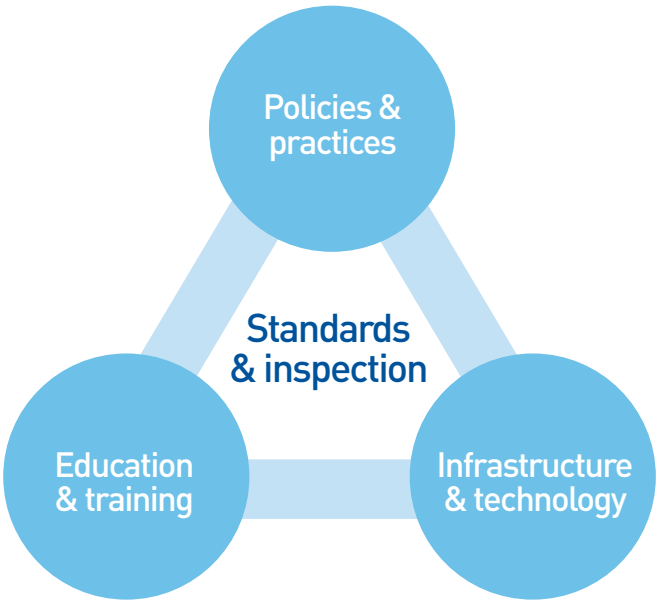
	Commercial	**Aggressive**	**Sexual**	**Values**
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting personal info	Being bullied, harassed 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 children receive e-safety education – where, how?

– Are staff – including support staff – 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

CEOP
REPORT ABUSE
THINK U KNOW
Directgov
Public services all in one place
www.direct.gov.uk
teachtoday
Childnet International
KnowITAll for parents
National Education Network
tda
department for children, schools and families

01/08-09/TWP0036/TT20777/15645/25K

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

www.becta.org.uk

Is your school **e-safe?**

Becta
leading next generation learning

Does your school...

- ☑ have a nominated e-safety co-ordinator?
- ☑ audit its e-safety measures?
  - **National Education Network** www.nen.gov.uk/esafety
- ☑ have a robust AUP?
  - **Becta** www.becta.org.uk/publications/aupsincontext
- ☑ use a Becta accredited supplier for internet services?
  - **Becta** www.becta.org.uk/schools/accreditedinternetsuppliers
- ☑ include e-safety measures in Section 4b of your SEF?
- ☑ keep an incident log and monitor your measures?
- ☑ handle cyberbullying issues well?
  - **Digizen** See www.digizen.org/cyberbullying
  - **Teachernet** www.teachernet.gov.uk
- ☑ raise awareness of the issues, e.g. through holding an assembly?
  - **thinkuknow** www.thinkuknow.co.uk/teachers

Do your learners...

- ☑ understand what safe and responsible online behaviour means?
- ☑ receive e-safety education at appropriate places across the curriculum?
  - **Signposts to safety** www.becta.org.uk/publications/signpoststosafety
  - **Kidsmart** www.kidsmart.org.uk
  - **thinkuknow** www.thinkuknow.co.uk/publications
- ☑ get the opportunity to improve their digital literacy skills?
- ☑ know the SMART rules?
  - **Childnet** www.childnet.com
- ☑ know how to report any concerns they may have?
  - **CEOP** www.ceop.gov.uk/reportabuse/index.asp

Do all your staff...

- ☑ understand e-safety issues and risks?
- ☑ receive regular training and updates?
  - **Childnet** www.childnet.com/kia
  - **thinkuknow** www.thinkuknow.co.uk/teachers
  - **Becta** www.becta.org.uk/schools/communities/safetynet
- ☑ know how to escalate an issue of concern?
- ☑ know how to keep data safe and secure?
  - **Becta** www.becta.org.uk/schools/datasecurity
- ☑ know how to protect themselves online?
  - **Teachernet** www.teachernet.gov.uk
  - **TeachToday** www.teachtoday.eu
- ☑ know how to conduct themselves professionally online?
  - **Every Child Matters** www.everychildmatters.gov.uk/resources-and-practice/IG00311
- ☑ know about the updated e-safety guidance for QTS standard Q21: Health and well-being?
  - **TDA** www.tda.gov.uk/partners/ittstandards/guidance_08/qts.aspx

Do your parents and governors...

- ☑ understand e-safety issues and risks?
  - **NGA** www.nga.org.uk/uploadfiles/documents/NGA-Becta%20Sept.pdf
- ☑ understand their roles and responsibilities?
- ☑ receive regular training and updates?
  - **thinkuknow** www.thinkuknow.co.uk/parents
- ☑ understand how to protect their children in the home?
  - **Know it all** www.childnet.com/kia
  - **thinkuknow** www.thinkuknow.co.uk/parents
  - **Directgov** www.direct.gov.uk

If not, why not?
Take action now!