

NGA/Becta Series No1

Being safe online



Technology and the online world offer endless opportunities for young people to learn, communicate, create, discover and be entertained. Earlier this year Becta launched the Next Generation Learning campaign to improve the use of technology in education and training.

Governors have a crucial role to play in ensuring that schools are using technology effectively, and that risks

are minimised. Becta is working closely with the NGA to help governors ensure the online safety of their pupils, and to raise awareness of the power and potential of Next Generation Learning.

Mike Briscoe - Director for Institutions, Leadership and Safeguarding, Becta.



This is the first in a series of four Becta inserts in our magazine. We are running this series because we are convinced that governors have an important role, both in promoting ICT and in ensuring that their schools make safe and effective use of the technology.

Why is technology so important and what are the benefits?

Over the past 25 years information and communications technology has developed into a powerful educational resource that is transforming the process of learning and teaching.

With a computer and internet connection – or even just a mobile phone – pupils can open the door to information, communicate with others or collaborate with learners on the other side of the world. Technology is being used to personalise learning, so that all pupils can progress, achieve and participate at their own pace.

When technology is used effectively, the results are inspiring – improved grades and retention rates, greater participation by students and increased productivity by teachers and tutors.

Phil Revell – Chief Executive NGA.

What's the issue?

Schools have the opportunity to transform education and help pupils fulfil their potential with ICT. But it's also important that pupils learn how to be safe when they are using these new technologies.

Governing bodies need to understand the implications of the use of ICT within their school and the need to provide suitable safeguards for pupils and staff.

Today's generation of school children are often referred to as 'digital natives'; born into a digital world, they have grown up with technology, but while the virtual world offers children huge opportunities, there are also

some risks. And while most children's confidence and competence in using technology is high, their knowledge and understanding of the risks may be low.

In most cases, the misuse of ICT is not serious and can be dealt with at classroom level. In rare cases however, the abuse of ICT can place individual children in serious danger and threaten the integrity of the whole school community.

Schools and governing bodies have a duty not only to teach pupils about safe and responsible behaviour using technology, but also to ensure that technical measures such as filtering and monitoring are in place to safeguard children, young people and staff.

What are the risks to children?

- When using the internet, children may be exposed to inappropriate content which may upset or embarrass them, or which could lead to their involvement in crime and anti-social behaviour.
- Some people use the internet to groom children with the ultimate aim of sexual exploitation.
- ICT offers new weapons for bullies who may torment their victims, for instance using websites or text messages.
- The recent surge in popularity of self-publishing and social networking sites brings new e-safety challenges, with many young people making available online some detailed – and sometimes inappropriate – personal information.
- While the internet offers new opportunities for doing business online, it also brings with it many unscrupulous traders to whom children and young people may be particularly vulnerable.

Cyberbullying

The new communications technologies have brought huge benefits to schools, but there are opportunities for misuse and abuse.

Cyberbullying is where children use text, email, websites and video to bully other children and sometimes even staff. This adds a new dimension to the problem of bullying; it is one of the most common threats to e-safety in schools today. This threat can be managed by schools and it is crucial that children and young people are taught how to handle such situations, and are made aware of the consequences - both in terms of the impact on the victim, and on the bully when the abuse is discovered.

- Cyberbullying can occur at any time and reach the victim when they are at their most vulnerable.
- The audience can be large and reached rapidly.
- People who cyberbully may attempt to remain anonymous.
- Cyberbullies may not match the profile or stereotype of the typical bully.

On a more positive note:

- It may be easier for adults to collect evidence about the bullying, from texts, emails or from monitoring software.

Focus – the Byron Review

Earlier this year Dr Tanya Byron, the renowned consultant clinical psychologist, published an independent review of the risks children face from the internet and video games.

The review set out an ambitious action plan for Government, industry and families to work together to support children's safety online and to reduce access to adult video games. Dr Byron set out three objectives:

Reduce availability – reduce the availability of harmful and inappropriate content, the prevalence of harmful and inappropriate contact and the conduciveness of platforms to harmful and inappropriate conduct.

Restrict access – equip children and their parents to effectively manage access to harmful and inappropriate content, avoid incidences of harmful and inappropriate contact and reduce harmful and inappropriate conduct.

Increase resilience – equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things, and parent effectively around incidences of harmful and inappropriate conduct by their children.

Child Exploitation Online Protection Centre

The facts

- 8m under-18s in the UK have internet access
- 2m have access in their bedroom
- 1 in 4 have met someone in the real world they first met online

Is your school protected?

Have you or your staff had a CEOP presentation?

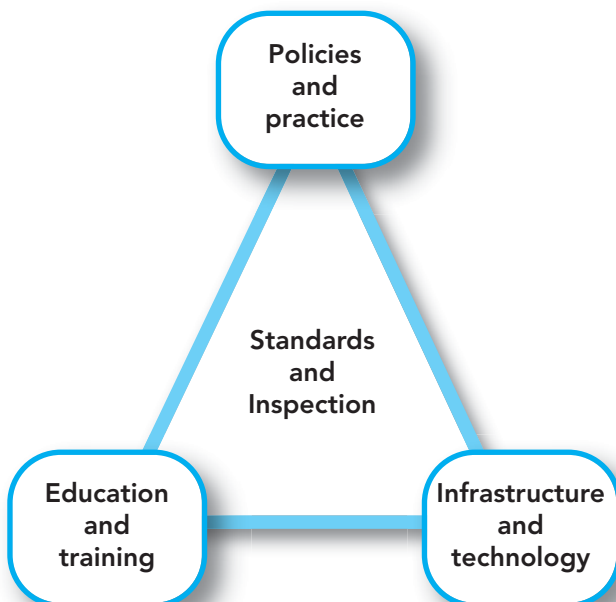


What should your school be doing?

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.

The underpinning model... PIES



Policies and practice

Does the school have a set of robust policies and practices?

Do you have an Acceptable Use Policy (AUP)? Are parents aware of it?

Does your anti-bullying policy include references to cyberbullying?

Are there effective sanctions for breaching the policy in place?

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 and how?

Are staff - including support staff - trained?

Do you have a single point of contact in the school for e-safety?

Do the leadership team and school governors have adequate awareness of the issue of e-safety?

Standards and Inspection

Do you monitor and review all of the above?

As a governor your role as a 'critical friend' is crucial to ensuring that schools are able to manage risk effectively in this area.

What can governors do to improve e-safety?

As a school governor we realise that, whilst you are dedicated to your school, you will also have a limited amount of time to deal with all the issues faced by your school.

Governors have a key role to play in ensuring that pupils at their school are able to take advantage of the huge benefits of learning with technology in a safe and secure way.

Dealing with e-safety can help to avoid significant gaps in child protection policies.

Here are some examples you may want to consider:

- Make sure you're aware of the benefits and risks involved in using technology in schools.
- Together with the leadership team, explore how the school would deal with potentially risky situations – such as pupils coming across inappropriate content, or children bullying each other using text or email.
- Think about appointing an 'e-governor' to lead on ICT.
- Work with your school to develop a clear strategy on ICT, which defines roles and responsibilities for management, implementation and safety, including the school's Acceptable Use Policy (AUP).
- Ensure resources are made available to provide a secure ICT system for the school, and to support e-safety training for children, parents, staff and, wherever possible, for the wider community.
- E-safety should be reviewed regularly in exactly the same way as other policies. You might consider publishing your e-safety policy alongside other school policies on the school website and in printed information to parents.
- The school's risk management strategy should consider the risk of breaches of ICT security.
- Staff and pupil disciplinary procedures should make it clear that abuse or misuse of ICT is a basis for disciplinary action.



Find out more

Next Generation Learning

More information on Next Generation Learning and on the issues discussed in this paper can be found on a dedicated website:

www.nextgenerationlearning.org.uk

NGA

The NGA website has an e-safety section with a pdf copy of this paper to download, and easy links to all the resources mentioned below.

www.nga.org.uk

The Byron Review

A copy of the review can be found on the DCSF website.

www.dcsf.gov.uk/byronreview

Childnet

In 2007 Childnet, commissioned by the DCSF, developed advice and guidance for schools on cyberbullying, including an award winning film. Resources on cyberbullying can be found on the Childnet website.

www.childnet-int.org

CEOP

Information about the Child Exploitation and Online Protection Centre's (CEOP) training and education programmes.

www.ceop.gov.uk

