Schools

January 2008

Becta leading next generation learning

Safeguarding children online

A guide for school leaders

www.becta.org.uk/schools/safety

Using technology safely

In the physical world it's relatively straightforward to work out what the duty of care towards the young people in your charge might mean, and the precautions you have to take.

The virtual world is more demanding, if only because the range of activities any of us can do online is expanding and changing. This is a good thing in itself, opening new opportunities for learning and creativity, but it also means thinking ahead of new risks. In this guide we'll set out the basic elements of good practice to keep our learners safe.

The changing face of e-safety

Consider the increasing mobility of information technology and you'll get a sense of how e-safety measures need constant new thinking. Where once the desktop computer was the only way to access the internet, now many mobile phones and games consoles offer broadband connections.

So young people may be working online in school, at home or perhaps a foster home, a library, an internet cafe, a youth centre, or maybe even a bus stop.

In any of these environments they may be working via the internet, or collaboratively within a closed network, or just with others in the room.

Against these possibilities you should set up effective security measures in the network. However, protecting young people (and all adult users) properly means thinking beyond this. Remember that they may have personal devices not covered by network protection and therefore the emphasis should be on getting everyone to understand the risks and act accordingly.

This means that designing and implementing e-safety policies demands the involvement of a wide range of interest groups:

- headteachers
- governors
- senior management
- classroom teachers
- support staff
- young people and parents or carers
- local authority personnel
- internet service providers (ISPs) and indeed regional broadband consortia, who are working closely with ISPs on network security measures.

"One time a friend was bullied online and she thought there was not a lot she could do about it so we got evidence of the conversations which were saved onto a computer, showed the vice principal, the bully was stopped."

Learner aged 14

All of these groups will have insights that help you set your school policies, and it is important that they are consulted. Policies of course are not enough. Everyone involved must have active practices that help young people and staff to identify and achieve safe behaviour. By involving all these groups from the start, everyone should feel the relevance of your policies and their personal responsibility for making them real.

Creating a safe ICT learning environment has four important elements:

- an infrastructure of whole-site awareness, responsibilities, policies and procedures
- an effective range of technological tools
- a comprehensive e-safety education programme for everyone in your establishment
- a review process which continually monitors the effectiveness of the above.

It should already be obvious that e-safety is a child safety – not an ICT – issue, and indeed it should not be managed primarily by the ICT team. It should be an extension of general safeguarding, and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying. Draw on technologists' expertise to get an accurate sense of the likely problems and their support in creating a solution.

Technology will certainly be part of the solution, and minimum defences are likely to include:

- virus prevention and protection
- monitoring systems to keep track of who downloaded what, when they downloaded it, using which computer
- filtering and content control to minimise inappropriate content via your network.

These measures are very necessary, particularly in this era of mushrooming social networking, where there are new concerns about the information children could be uploading to internet sites, and the risks to which they could be exposed as a result.

"A letter has gone out to all parents, both as a 'please be aware this is what we're doing as a school to be aware of online safety', but also as a prompt for the parents to ensure they have got all the parental controls in place at home, and are being as vigilant in the home as we are in school."

Parent/Governor

Becta supporting e-safety

Safeguarding children and young people in both the real and virtual world is everyone's responsibility.

Any establishments relying solely on technological solutions could be placing themselves, and their pupils and staff, at risk.

Children need to be safeguarded wherever and whenever they are online.

National Education Network

Although ultimate responsibility for e-safety must lie with each school or establishment, at Becta we're concerned to ensure that work at a national level should support those localised needs.

E-safety is a fundamental consideration in the framework of functional, technical and service quality standards that underpins the National Education Network. As the network management authority, we engage with service suppliers to ensure:

- a clear definition of the minimum level of filtering (currently defined within our ISP accreditation scheme)
- thorough on-site testing and quality assurance of services
- agreement to action plans where services do not meet requirements
- monitoring action plans until services meet required minimum specifications.

ISP accreditation

Our internet services accreditation scheme enables providers of internet services to education (including commercial suppliers, Regional Broadband Consortia and local authorities) to demonstrate how their offerings meet or exceed Becta's minimum requirements.

To be accredited, suppliers (who will have voluntarily submitted their services for evaluation) must be able to meet and maintain specific standards in content filtering and service performance.

At the same time we provide clear information about the basic technical features that should be in place if you are looking to purchase internet services, or want to check how your current services relate to these requirements.

The scheme means that the requirements are not only met, but are constantly monitored and maintained to ensure service excellence and best practice.

"If someone goes on a chatroom being rude or something you can just tell your parent and if you're on MSN you can block them or delete them."

Learner aged 8

Becta Accredited Internet Services

What you should be doing

- Use a whole-establishment approach towards responsibility for e-safety.
- Develop an acceptable use policy (AUP) detailing the ways staff, pupils and all network users (including parents) can and cannot use ICT facilities.
- Sample AUPs are available both online and via local authorities. Tailor them to fit your own circumstances.
- Link AUPs with other school policies, such as anti-bullying and guidance on copyright and plagiarism.
- Designate a senior management team member with responsibility for safeguarding to also be the central contact point for all e-safety issues.
- Headteachers, supported by governors, should take the lead in embedding the agreed e-safety policies in practice.
- Ensure the young people in your charge are aware of potential risks and how to practise safe, responsible behaviour, wherever and whenever they are online.

Your e-safety strategy should:

- allow young people to develop their own protection strategies for when adult supervision and technological protection are not available
- give information on where to seek help and how to report incidents
- help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online
- provide guidelines for parents, carers and others on safe practice
- ensure you regularly monitor and review your policies with stakeholders
- ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.

Above all, e-safety education should be a continuing feature of both staff development and young people's educational lifelong learning.

Further information

Becta's website highlights the safety issues and provides advice on how to use technology safely
www.becta.org.uk/schools/esafety

There are a number of Becta publications available from our website including:
'E-safety: Developing whole-school policies to support effective practice' and 'Signposts to Safety' (Primary and Secondary versions)
www.becta.org.uk/publications

For information about the Becta accreditation of internet services to education scheme
www.becta.org.uk/schools/ispsafety

There is also a mailing list – Becta Safetynet, where you can exchange information with your peers about e-safety issues
http://lists.becta.org.uk/mailman/listinfo/safetynet

Millburn Hill Road
Science Park
Coventry CV4 7JJ

Tel: 024 7641 6994
Fax: 024 7641 1418
Email: becta@becta.org.uk

www.becta.org.uk

01/DD07-08/150/BX/5k

The raw material for this paper is sourced from fully certified sustainable forestry and is fully recyclable.