

Guidance to educational establishments on Child Protection and the use of the Internet

From the Cambridgeshire Education Child Protection Service
and Education ICT Service
Updated January 2007

Produced By:	Paul Springford
Reviewed By:	Mazzie Bartimus
Team:	e-learning
Date:	29 January 2007
Version	1.0



This document is available in electronic format on the Cambridgeshire Education Portal (resource id 2143)

Introduction

- The government, local authorities and schools are encouraging the use of the internet to promote learning in a wide range of areas. Exploiting the online world is now a key means of extending and personalising the educational experience of all learners. Young people hardly need to be persuaded to learn in this way.
- School governors, including the headteacher, share with the head of local authority children's services personal responsibility for the safety of their school's children and young people. This responsibility extends to safe use of online facilities provided by the school.
- It is recommended that a member of the senior leadership team is designated as Internet Safety co-ordinator.
- This document will refer to schools and teachers. However, the guidance contained here is applicable to many other Education settings, such as After-school Clubs, Youth Clubs and Libraries, and to all adults who supervise children in these settings and are responsible for their welfare.
- This guidance focuses on the personal safety and well being of pupils in your school. It sets out a number of points to clarify the potential risks and steps that staff can take to minimise those risks.
- This document is principally concerned with safe use of the internet and considers the content children are uploading as well as what they are downloading. The use of other technologies, notably mobile phones, increasingly overlaps with computer-based online activity. In these situations the principles of awareness and managing risk expressed in the guidance continue to be relevant.
- A separate document, Guidance on Access and the Safe Use of School IT Equipment, advises on deterring misuse of ICT and access to improper material, particularly by adults in schools. It also advises on appropriate action if there is a suspicion that such misuse has occurred. It is available on the Cambridgeshire Education Portal (resource id 3044).

Your Teaching Programme

- Learning to use the resources of the internet safely and appropriately is an important part of the education of all pupils. Schools should incorporate Internet Safety into the curriculum.
- It is advisable to share with parents the steps that the school is taking to promote internet safety and to involve them in discussion about what constitutes safe use both at school and at home. Written communication with parents and carers can be helpful, and events at school, possibly with professional input, are often more effective.

Acceptable Use Policies

- Adults and children working in schools should observe an Acceptable Use Policy (AUP). It should normally be shared with parents. It may be part of a broader AUP covering the use of all the school's ICT facilities.
- Where children are involved in the development of an AUP, schools generally find that there is better understanding of the issues and enforcement is made easier.

Bullying and Abuse

- All of the communication systems referred to in this guidance can be misused to offend, upset or intimidate pupils or staff both in school and outside. This is sometimes described as cyber-bullying. It can include sites which invite users to "rate" other people.
- Schools need robust policies to deal with any incidents and cyber-bullying should be covered in any anti-bullying work which is undertaken.
- Offensive and intimidating messages must not be deleted, since it may be possible to trace the sender.

Internet Service Providers

- All schools should be using a filtered internet feed from an education-accredited Internet Service Provider (ISP). In Cambridgeshire, this will normally be via the Cambridgeshire Community Network (CCN). The internet feed for CCN schools is provided by our regional broadband consortium, E2BN, and web-filtering is achieved using the Protex system.
- Any school making alternative arrangements for internet provision must ensure and be able to demonstrate that it meets the Becta standards for accredited internet providers.

Safe Use of the Worldwide Web

- To provide safer access to web pages, Protex offers a number of different “profiles”; these are customised filtering regimes designed for different groups of users. Currently E2BN offers four profiles:
 - primary
 - middle
 - secondary
 - staff

It is possible for schools to move groups of users to different profiles at any convenient time, either by changing the settings on specific computers, or by changing the policies for specific users. These changes must only be made by a technically competent person properly authorised by the headteacher.

- Protex categorises web sites in three ways:
 - some URLs (addresses) are permanently blocked
 - some are trusted - e.g. BBC and government sites – and this includes all files which can be downloaded from the site
 - some are content-checked before being allowed
- Staff who believe that an inappropriate item has passed through the filter should report it to the Schools ICT Helpline, by phone if the matter is urgent (0845 045 0973). Non-urgent queries can be sent to ict.helpline@cambridgeshire.gov.uk When Protex blocks web pages, an information page is displayed, and this includes a teacher’s button enabling a comment or a request for unblocking to be submitted.
- Some schools may wish to purchase their own Protex server in order to accommodate a different range of profiles from those offered centrally by E2BN. This option will have implications for budgets and management time, and is most likely to be pursued by larger schools. Schools may also choose to use a third-party filtering system locally. Schools taking up either of these options will receive the Staff profile and then derive their local profiles from that.
- It is crucial for staff to understand that a filter can reduce but not eliminate the risk of exposure to inappropriate material on the worldwide web. Teachers should be aware of appropriate strategies for supervision, for example by suitable positioning of computer screens, and pupils should know the school’s procedure for reporting any encounter with inappropriate words or pictures. In larger schools, auditing systems, which record every webpage visited by individual users, can help to promote sensible practice.
- Because of the huge scale of the internet, many people use search engines to help them find relevant material. Often, an innocent search can result in offensive or adult sites being listed, and even if the filtering system prevents the user from following a link to the site in question, sufficient information can be displayed in the search results to upset or offend, or encourage access later on an unsupervised computer. Learners, especially younger pupils, should be encouraged to use search tools such as Yahoo!igans, which search across a restricted set of websites with educational relevance.
- Google is a popular and effective search engine and can be useful for restricting searches to UK sites or for finding images. The Protex service will allow schools to use Google more confidently. It will enforce the Very Safe Search option, and in Google image searches it will prevent the display of thumbnail images from blocked sites.
- While many schools help pupils to locate information efficiently by teaching a programme of information skills, it is also important that pupils learn to identify the origin of pages they find in order help them evaluate the point of view and reliability of the author. This can involve analysing the URLs of webpages and using other tools to obtain information about the website on which they are found.

- Pupils should be taught to check with their teacher before providing any personal information that may be requested by a specific website. They should understand that they must only supply minimal untraceable details, such as a first name, to an enquiring website and must never divulge anyone else's personal information.

Publishing Information on the Internet

- The most serious risk to pupils using the internet involves the possibility of someone being hurt, exploited or abused as a result of personal information being disclosed online. Pictures, names, addresses, ages or information about a child's likes or dislikes can be used to trace, contact and meet a pupil with the intention of causing harm.
- The risk to children may not be immediate, since there can be a long period of building up a relationship, known as the 'grooming process'.
- On no account should either first names or surnames be attached to photos of children on websites. Care must be exercised that the filename of a photograph (e.g. janesmith.jpg) does not inadvertently identify a child.
- School websites should not include close-up pictures of children. All photographs of children should be general. Photos should be taken in such a way as to ensure that the individual identity of a child is protected (e.g. from an angle, in profile, at a distance.) If a website includes a child's photo, it could be downloaded from the web and edited in an unpleasant or embarrassing way.
- Before any pictures or examples of pupils' work are published on a website, written permission from parents or carers must be obtained. Efforts should be made to ensure that they understand the implications before giving permission.
- Staff and pupils with Starz or Digitalbrain user accounts can publish pictures and other information on the Cambridgeshire portal, specifying whether it is available to the public at large or restricted to a specified group of account holders. Parental permission and understanding are still required, and it is important that staff are equipped to apply access restrictions securely.

Using E-mail and Online Discussion

- Users can send and receive messages and attached files, either privately by e-mail or publicly in a discussion group or forum. These groups make it possible to follow a global discussion between a number of people.
- E-mail and discussion groups provide an environment where close relationships can develop quickly, without a check of the new contact's integrity or intentions. It is possible for people to conceal their real identity, for example by pretending to be younger than they really are.
- The apparent privacy of e-mail means that it is relatively easy for a stranger to make contact with a child without any one else's knowledge. The biggest risk is that a pupil might send something that reveals traceable information about them. There is a chance that an undesirable person could see this, contact the pupil and cause them harm.
- It is essential that supervising staff can monitor all e-mails sent and received by pupils, and that pupils are aware that this is possible. Free services such as Hotmail do not allow this, and often carry unsuitable advertising. Teachers should understand e-mail 'headers' since this is helpful if there are reasons to question the origin of an e-mail. For pupils with Starz or Digitalbrain accounts, the Safemail option allows teachers to confine pupils' ability to send and receive e-mails to a pre-determined list.
- Staff who communicate with children by e-mail should only send messages from and to the official accounts provided by their schools, since these can be audited if there are any suggestions of misuse.
- Detailed safety guidance for schools with Starz accounts is published in the teachers area on the Starz website.
- Schools should ensure that only appropriate discussion groups are available to pupils. For pupils with Starz or Digitalbrain accounts, online discussions can be set up with membership controlled by a teacher.
- Pupils should know whom to inform if they receive abusive or unwanted messages of any kind. The school's approach to a pupil or adult who sends inappropriate e-mails or messages should be clear. It must be seen to be effective in halting such practice.

Chatrooms

- Chatrooms enable users to engage in 'conversations' with people across the street or across the world. They are similar to telephone conversations except that messages are typed instead of spoken. Usually everyone in a chatroom can see all the other participants' contributions. Unlike email, once chat sessions are finished there will often be no obvious record of what has been posted.
- Schools often see chatrooms as a home-leisure pursuit. However, the role of chatrooms in schools is likely to change, using systems such as Starz or Digitalbrain which allow teachers to set up secure chat sessions where they can control who is taking part and when they occur.
- The danger to children of public chatroom use is that people do not necessarily tell the truth about who they are. If children provide personal information it is possible that they could be traced and contacted by another user who could then cause harm.
- Personal safety programmes used in schools should explore with pupils the potential dangers of using chatrooms so that children understand how they can protect themselves. Most special and secondary schools in Cambridgeshire have received a pack called Chat Safe, produced by the Police, with guidance for young people and their families.

Social Networking

- Social Networking areas are websites which help connect friends using a number of tools like blogs, profiles, internal email systems and photos. Well known sites include Bebo and Myspace. They can be customised, and pictures, video and music can be uploaded and shared. They can bring users into contact with strangers by developing networks of "friends of friends".
- While children may not be using these sites in school, they are increasingly likely to form part of their out-of-school life, and personal safety programmes should take account of this. Sharing inappropriate information and images could prove embarrassing and even dangerous. Children using these sites should understand how to control levels of access to their own space.

Online Learning Platforms

- Many schools and educational organisations are providing opportunities for pupils to use websites with controlled access such as Starz and Digitalbrain. They are sometimes called online learning environments or online learning platforms. These systems offer many easy-to-use communication and collaboration tools enabling online communities to be created with a restricted membership. DfES expect all schools to offer pupils a personal online space using an approved learning platform by 2007/8.
- These online systems are attractive to schools because they offer a measure of security by restricting access to authorised members. A number of facilities such as web-publishing, e-mail, online discussion and chat are available, generally with an increased level of safety compared to completely open use of the internet.
- While these systems do provide a more secure environment than the open internet, teachers and pupils still need to adopt a careful approach and be aware that abuse is possible. Personal information must not be divulged, and pupils should know whom to inform if they receive unwanted messages. Membership of an online community should only be granted to those who are known to have genuine justification, and a code of conduct for users should be known to everybody. Where users are allowed to make material available on the open internet, they should ensure that safety has been fully considered and that appropriate permission has been given. Schools must ensure that staff responsible for allocating passwords and levels of privilege to users understand the process fully and do not prejudice pupil safety by thoughtless management of the system.
- Schools should understand that the levels of security on the Starz and Digitalbrain systems do not at present warrant the storage or transmission of highly sensitive or confidential information.
- More detailed guidance on safety options for Starz and Digitalbrain users, including home access issues, is provided separately to subscribers with pupil accounts.

References:

- <http://www.ccceducation.net> - Cambridgeshire Education Portal

Official sites

- <http://www.becta.org.uk/schools/esafety> - *Becta's E-safety* site: the principal national site for information and guidance on safety online.
- <http://www.thinkuknow.co.uk> - the *Child Exploitation and Online Protection Centre (CEOP)* site aimed at children and young people - for advice on online safety and for reporting grooming and abuse.
- <http://www.iwf.org.uk> - the *Internet Watch Foundation*, for reporting illegal online content, especially images of child abuse.
- <http://www.parentscentre.gov.uk/usingcomputersandtheinternet/> - ICT section of the *DfES Parents' Centre* website with information and advice about online safety.

Recommended resources

- <http://www.gridclub.com/cybercafe/teachers> - homepage for the *Internet Proficiency Scheme* developed to help teachers educate KS2 children on staying safe on the Internet.
- <http://www.childnet-int.org/kia/> - for information about *Know IT All*, a set of interactive resources developed by Childnet to educate young people, parents and teachers about safe and positive use of the internet and distributed to all secondary schools in November 2005 on CD-ROM.
- <http://www.bbc.co.uk/cbbc/help/safesurfing/> - *Stay Safe*, the online safety area of the CBBC website.
- <http://www.websafecrackerz.com/> - *Websafe Crackerz*, a game-based online safety site for young people.
- *E-safety: Developing whole-school policies to support effective practice* can be ordered or downloaded from the publications section of the Becta website - <http://becta.org.uk/corporate/publications/>.

Staying Safe is the Personal Safety Programme produced by and available from the Cambridgeshire Education Child Protection Service (tel. 01223 712092). It contains useful information and resources to teach children about personal safety skills.

Curriculum materials on the issue of Internet Safety can be found as part of the Personal Safety Units in the Secondary Personal Development Programme. These lessons are intended to encourage pupils to explore some of the risks involved in using the Internet, balanced with some of the benefits. Information about these resources is available from the PSHE Service (01480 375171).