

## **E Safety**

### **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, and to young people, this is an obvious and natural way to learn.

This document provides guidance to schools on the safe use of the Internet and considers the content children are uploading as well as what they are accessing and 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.

This guidance focuses on the personal safety and well being of pupils in your school. It clarifies the risks and the steps that staff can take to minimise those risks. The guidance refers to schools and teachers; however, it applies equally to many other Education settings, such as After-school Clubs, Youth Clubs and Libraries, and to the whole children's workforce. There are other risks associated with the use of the Internet and communications devices that are not covered here, e.g. phishing (acquiring personal and account details by deceit for use in fraud and identity theft) and messaging scams (mobile phone messages that connect you to premium rate services). Schools may wish to include these in education programmes.

The Headteacher and School Governors share personal responsibility for the safety of their school's pupils with the head of the local authority children's services. This responsibility extends to the safe use of online facilities provided by the school. We recommend that a member of the senior leadership team is designated as Internet Safety co-ordinator.

### **Your Teaching Programme**

It is important that pupils of all ages learn to use the resources of the Internet safely and appropriately. Schools should incorporate Internet Safety into the curriculum, most likely through the PSHE curriculum with reinforcement across the curriculum, notably in ICT.

Parents should be informed of the steps that the school is taking to promote Internet safety and should be involved in discussion about what constitutes safe use both at school and at home. Written communication with parents and carers can be helpful, but events at school, possibly with professional input, can be more effective.

### **Acceptable Use Policies**

An Acceptable Use Policy (AUP) should be observed by adults and children working in schools. 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 that 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 Milton Keynes, this will normally be via the Schools Broadband Network, managed by the Open University. The internet feed for Milton Keynes Schools is currently obtained from a combination of commercial providers (Affiniti and Easynet) and the Joint Academic Network (SuperJANET). Web-filtering is achieved using the KidGuard system managed by the Open University, which also allows schools to customise their filtering through the use of black listing and white listing. The filtering system in use is kept under constant review and may be subject to change.

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.

Note: School administration computers, provided by and supported by HBS, are connected to the Internet via the Milton Keynes Council corporate Internet connection and use a different filtering system.

### **Safe Use of the Worldwide Web**

It is crucial that staff 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, e.g. by suitable positioning of computer screens, or by network based screen scanning software (e.g. ranger)

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 later access on an unsupervised computer. It is important that learners are taught how to search the web effectively and efficiently so that there is less incidence of finding inappropriate sites. Younger learners can be encouraged to use search tools such as Yahoooligans, which search across a restricted set of websites with educational relevance.

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 web pages 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. This is to secure their personal safety as well as to prevent identity theft and fraud.

Google is a popular and effective search engine and can be useful for restricting searches to UK sites or for finding images. The Milton Keynes broadband service allows schools to use Google more confidently. It enforces the 'Very Safe Search' option, and in Google image searches it will prevent the display of thumbnail images from blocked sites.

### **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'.

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. 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.

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.

### **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.

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.

Schools should ensure that only appropriate discussion groups are available to pupils.

Pupils should have clear guidelines about what to do 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.

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.

Schools often see chatrooms as a home-leisure pursuit; however, the role of chatrooms in schools is likely to change. Systems exist which allow teachers to set up secure chat sessions where they can control who is taking part and when they occur.

Personal safety programmes should explore with pupils the potential dangers of using chatrooms so that children understand how they can protect themselves.

### **Social Networking**

Social Networking areas are websites which help connect friends using a number of online tools such as blogs, profiles, internal email systems and photos. Well known sites include Bebo and Myspace, and they are very popular with pupils. 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. 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 a personal online space to be available to all pupils by Spring 2008.

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.

### **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.
- <http://publications.becta.org.uk> – Essential reading. A search for e-safety will produce some excellent publications which can be ordered or downloaded from the publications section of the Becta website.

### **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.

## **Glossary**

**Downloading:** To receive data from the internet or any other remote system. This definition includes files that a user actively chooses to receive and store (as in “he downloaded an mp3 file”), but also includes any other information that is viewed or listened to, such as web pages, images on web pages and emails. Most downloads are usually tracked and recorded on the user’s computer, on local networks and on the sender’s server.

**Uploading:** To send data to a website, the internet or any other remote system, usually to enable others to view them. This includes files such as web pages that are placed on servers for others to download, but also, for example, blog or forum postings and information in registration forms on web sites. Most uploads are not usually tracked or recorded on the user’s computer or local networks.

**URL:** The address of a web page or any other file on the internet. <http://www.mkconnect.org.uk/> is an example of a URL.

**Blog:** A blog (short for web log) is a website where the author(s) posts entries which are usually available for anyone to read. Readers are encouraged to add their comments to each main post.