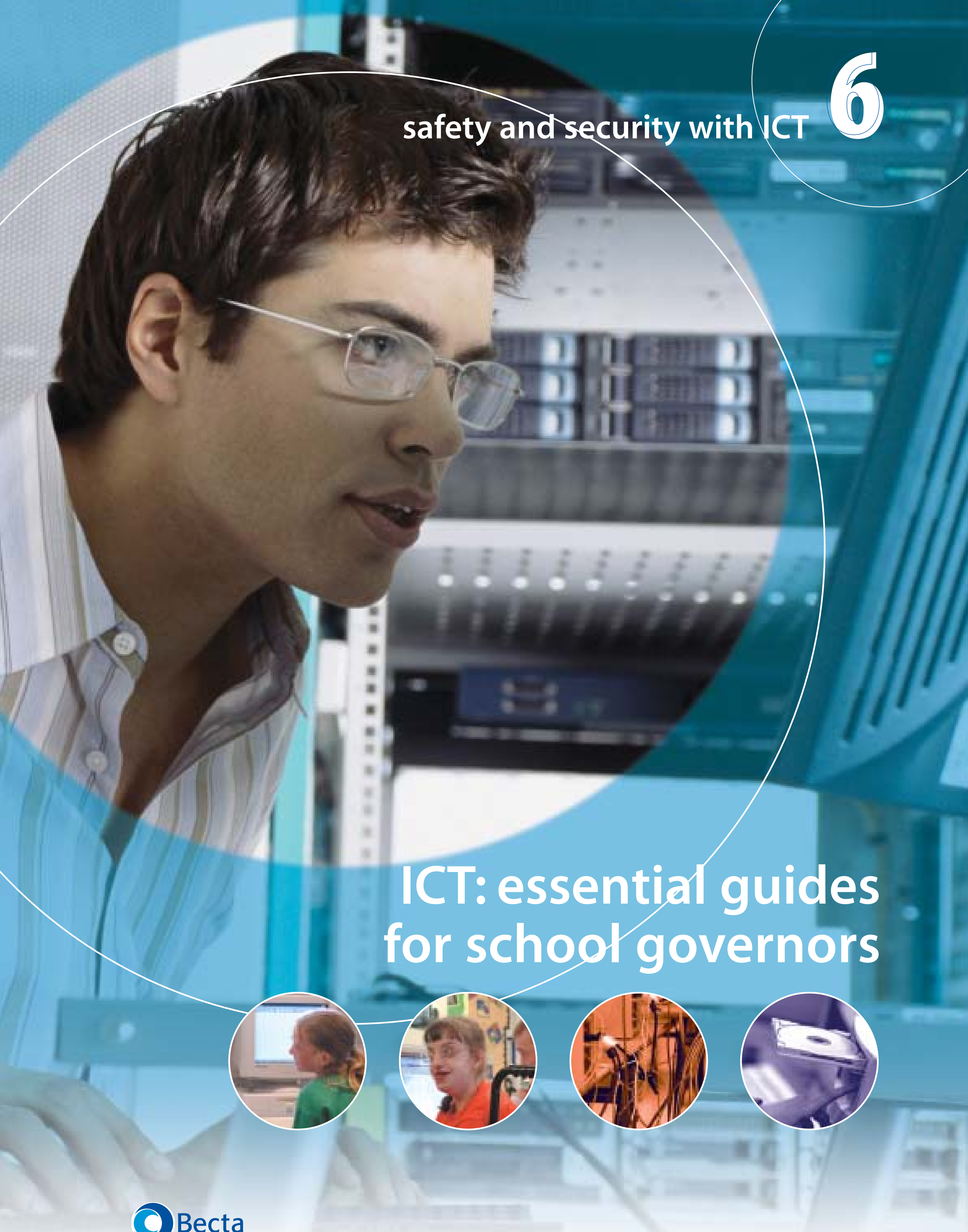


safety and security with ICT 6

ICT: essential guides for school governors

Becta
ICT Advice

This is one of a series of documents for school governors produced by Becta. This guide outlines the need for governors to monitor the use of ICT – and pupils' use of the internet in particular – so that while pupils use ICT whenever and wherever it is appropriate, they do so in safety. It also highlights the main health and safety issues associated with using ICT equipment.

Taking responsibility for the use of ICT

ICT and the internet are powerful educational resources that are transforming the process of learning and teaching in schools and across the community. With a computer and internet connection – or even just a mobile phone – pupils and adults alike can gain access to a vast amount of information and communicate and collaborate in a variety of ways.

Not all information available via the internet is accurate, or even legal, however, and schools have a duty to teach pupils about safe and responsible behaviour using technology. Governing bodies have a duty to understand the implications of the uses of ICT within schools and the need to provide suitable safeguards for pupils and the school.

The role of the governing body

There is no formal requirement on governing bodies to develop an ICT strategy or to consider ICT safety and security issues. However, the safe and secure use of ICT has an impact on a number of areas of statutory responsibility for governing bodies, including Health and Safety Policy, Child Protection Policy and legal requirements for data protection and freedom of information.

Data Protection Act (1998)

Information held by schools on children and adults can only be used for specific purposes. The Act requires schools to notify the Office of the Information Commissioner of:

- the purposes for which the school holds personal data
- what data it holds
- the source of the data
- to whom the data is disclosed
- to which countries the data might be transferred.

Individuals have the right to access information about themselves held on computer files and some paper files under the Act.

Freedom of Information Act (2000)

This Act provides the public with the right to gain access to 'recorded' information held by public bodies such as schools. All schools are expected to produce a 'publication scheme' that outlines their publicly available information (it should be noted that there are a number of exemptions).

Becta's *Data protection and security for schools* publication provides an overview of the implications of recent legislation. [**http://www.becta.org.uk/corporate/publications/publications_detail.cfm?currentbrand=all&pubid=136&cart=**]

Good practice suggests that all schools should actively consider ICT safety and security and that they should take the following steps:

- Governors should develop an awareness of the issues and risks of using ICT in schools alongside the benefits. Schools could consider appointing an 'e-governor' to lead on ICT including safety issues
- Governors should expect the 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)
- Resources should be made available to provide a secure ICT system for the school and to support internet proficiency training for children, parents, staff and, wherever possible, for the wider community
- Internet/ICT safety should be reviewed regularly as part of the review of the school's health and safety and child protection policies. It is suggested that the annual report and school prospectus should contain a summary of the school's policies on ICT safety for the benefit of parents
- The school's risk management strategy should look at the risk of breaches of ICT security and how these should be dealt with both for pupils and for staff
- Staff disciplinary procedures should cite the serious misuse/abuse of ICT as a basis for disciplinary action.

Creating a safe and secure environment for ICT

All schools want to create a safe and secure ICT learning environment but many are unsure how to begin. There are three components that schools need to establish:

- An infrastructure of whole-school awareness, responsibilities, policies and procedures
- A secure ICT system
- A comprehensive internet safety education programme for the whole school community.

Whole-school awareness

There is a need to raise awareness of ICT safety throughout the school. It needs to be stressed that this affects every member of the school community, including the governing body.

All schools should put in place overall policies for the reasonable uses of ICT, such as an AUP. Sample policies are available, online and via LEAs, which schools can use as a basis for their own policies. An effective internet safety policy needs to be tailored to the individual needs of the school, and is as much about an understanding and consideration of the issues as having a written policy document. The policy should be developed in consultation with all key stakeholders, including parents and children, so that there is an understanding of the issues and the safeguards across the school community.

Secure ICT system

All staff and pupils need to observe 'simple, everyday' security measures such as not sharing password information, teachers logging out of MIS software and not leaving their computers unattended, and regular backing up of vital assessment data.

There are a range of tools that schools can use to make their ICT system secure:

- **Firewall and virus protection** to prevent unauthorised access to the school's network. A firewall can prevent information about pupils and the school being seen by unauthorised users and protect computer systems and files from viruses that can corrupt or destroy important information. The governing body should ensure that a suitable firewall is in place
- **Software filters:** different types of filters are available to restrict access to inappropriate websites and some schools go further by subscribing only to collections of websites that have been vetted and approved for access by children. Schools should monitor the use of ICT on a regular basis, by keeping track of information accessed and/or downloaded from the internet to check its suitability
- **Using an accredited ISP:** Becta's advice is for schools to only access the internet through an accredited Internet Service Provider (ISP). Check with your LEA or RBC or see **http://ispsafety.ngfl.gov.uk**
- **Awareness of wireless technology issues:** an open access wireless system allows 'eavesdroppers' to select and copy any/all transmitted data. Simple encryption systems are available which will maintain security against the majority of 'hackers'
- **A clear policy on using personal devices:** as increasing numbers of pupils and staff use laptops, memory sticks and other portable storage devices on the school network, there needs to be a policy regarding their use, to protect the school network from viruses and inappropriate access to sensitive data.

Internet safety education programme

By being informed of the issues and potential risks, users of the internet – pupils and staff – can take measures to protect themselves and recognise when the benefits of the internet become endangered. Becta has developed an Internet Proficiency Scheme which aims to help Key Stage 2 children to learn how to use ICT responsibly and safely and 'Signposts to Safety' is a new publication for pupils at Key Stages 3 and 4 [**http://www.becta.org.uk/corporate/publications/publications_detail.cfm?currentbrand=all&pubid=194&cart=**].

Internet Proficiency Scheme for Key Stage 2

The aims of the scheme are to:

- develop a set of safe and responsible behaviours for pupils to adopt when online
- support the skills, knowledge and understanding as set out in the National Curriculum Schemes of Work for Citizenship and Personal, Social and Health Education (PSHE)

The teaching pack can be downloaded from the Internet Safety site. [**http://safety.ngfl.gov.uk/schools/index.php3?S=3**]

Copyright and software licensing

Copyright is part of a set of legal rights and regulations defined in the Copyright, Designs and Patents Act (1988). These rights are called intellectual property rights (IPR).

Governors should be aware that all electronic materials, including digital images, computer programs and text, are covered by IPR. IPR also applies to electronic materials accessed through such formats as CD-Roms and web pages.

When using electronic material in another context, such as printing copies of an image or worksheet for classroom use, the copyright situation should be ascertained. Absence of copyright information or the fact that a particular type of use is not mentioned does not constitute permission. Further information on copyright and software licensing is available on the ICT Advice website [**http://www.ictadvice.org.uk/indexphp?section=ap&rid=436&catcode=as_pl_leg_03**]

Identifying the risks

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.

Risks to children

These can be summarised as communication with inappropriate people, or access to age-inappropriate material.

Exposure to the threat of physical danger and abuse
This is the most worrying risk associated with the use of the internet. A criminal minority make use of the internet and related services such as chat rooms to make contact with young people. These techniques are known as 'online enticement', 'grooming' or 'child procurement'. The Sexual Offences Act 2003, which came into force in May 2004, includes a grooming offence specifically introduced to combat this misuse of the internet.

There is a risk that, whilst online, a young person may provide information that can identify them, or arrange to meet someone they have communicated with online. The governing body needs to ensure that every effort is made to educate pupils regarding these issues. Often, of course, pupils are at most risk outside the school environs, so where possible, advice should be supplied to parents and the local community.

A new arena for intimidation and bullying
New methods of communication open up opportunities for intimidation and bullying, by text message or instant messaging services, by email, or within chat rooms. Regrettably, there are also abusive or discriminatory websites that target vulnerable children. Becta has produced guidance on how schools can address these forms of bullying [**http://www.safety.ngfl.gov.uk/schools/document.php3?D=d65**].

Misuse of resources
Electronic access to a wealth of information and imagery brings with it the danger of assignments and projects being copied from the internet or from a CD-Rom; at best, this may mean that children have no real grasp of the material they are appropriating, at worst it may mean they are guilty of plagiarism and cheating.

Access to unsuitable and inappropriate materials
There is a risk that, when using the internet, email or chat services, young people may be exposed to inappropriate material which encourages activities that are considered unhealthy, dangerous or even illegal.

Research

In 2002 Becta commissioned an 'Audit of Internet Safety Practices in English Schools' which investigated and reported on current practices in teaching internet safety.

Findings included the fact that schools tended to rely heavily on supervised internet access, often ensuring that pupils only visited websites recommended by the teacher. This may lead both to a lack of awareness of good internet safety practice when surfing the internet outside school and a lack of emphasis on developing search and evaluation skills.

[**http://www.becta.org.uk/research/research.cfm?section=1&id=2748**]

Risks to the school

Viruses
Viruses can cause disruption and damage, often incurring expense, to computer networks. It is essential that schools put in place comprehensive security systems that can protect against unauthorised access and accidental damage.

Unauthorised access
Schools generate information and store data, only some of which may be intended for a wider audience. The governing body should check that suitable storage and back-up systems are in place. The Data Protection Act (1998) and the Freedom of Information Act (2000) control the uses of information produced by schools.

Schools publish information in prospectuses, reports and on websites that showcase the school. Such websites must protect the identity of children and if, for example, photographs of children are to appear, permission from parents or carers must be obtained and care taken not to provide information that could be misused.

Case Study

The Bliss Primary Charity School, Northamptonshire provides individual email addresses to pupils through an educational portal service which allows them to be part of a secure and controlled online learning community. The web-based email system offers automatic filtering, virus checking and other security features. Age-appropriate content is carefully selected and access to interactive areas is based on peer groups. Pupils are only allowed to send and receive emails under supervision. Using their password, pupils can log on from their home computers and parents are encouraged to take a close interest.

Pupils are taught never to reveal personal details in messages and to report anything that upsets them. Teaching staff have access to all passwords and regularly monitor emails sent and received from both school and home. Pupils' email addresses incorporate the child's first name only and the school's domain name. [**http://safety.ngfl.gov.uk/schools/document.php3?D=d30**]

Health and Safety

Teachers and pupils are not specifically mentioned under any UK health and safety regulations or EU legislation with regard to ICT. However, the regulations should be interpreted to include teachers who use computers in their work, together with all non-teaching staff who are covered specifically by the regulations. Employers must ensure that risk assessments are made and put in place to manage any identified risk. In the case of schools, the employer (the LEA, education authority or governing body) should provide health and safety policies and should ensure that schools put these into operation.

In practice, it is often the headteacher or classroom teacher who holds the day-to-day responsibility to ensure that ICT equipment is used correctly and safely. Where pupils are allowed to connect or unplug electrical equipment, this should only be after proper instruction and always under the supervision of a teacher.

Inclusion

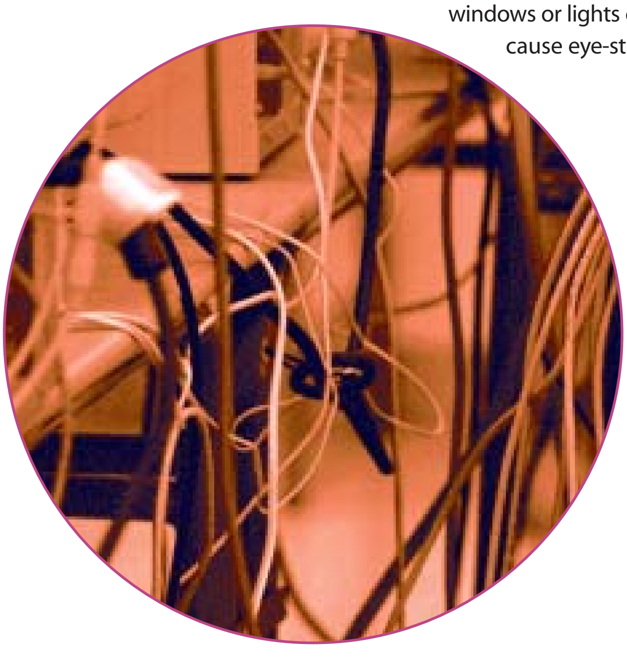
In particular, the governing body should be aware that some pupils are more vulnerable than others, particularly those with special educational needs.

- General advice to 'never go with strangers' needs to be extended to virtual friendships too
- Access technologies need to be professionally positioned and secured, especially for wheelchair users
- Pupils who need technology to access the curriculum need to take regular breaks away from the computer
- Trailing wires present a particular hazard if pupils are visually impaired
- Both pupils and equipment need to be safeguarded where behaviour is an issue.

Issues to consider

The use of ICT equipment has caused concerns with, for example, Repetitive Strain Injury (RSI), eye strain and related problems caused by stress and working with Visual Display Units (VDUs). Care and attention to the design and layout of the working area can help to overcome these problems. Other issues, such as general office safety, relate more to the working environment but can be applied to the classroom or library environment. The physical security of all ICT equipment also needs to be considered.

Monitors, keyboards, interactive whiteboards, printers and other ICT equipment such as photocopiers need to be certified annually for electrical safety. Most ICT equipment generates heat and noise, so care should be taken to locate it in well-ventilated areas; avoid siting where glare from windows or lights could cause eye-strain.



Governors should ensure that furniture purchasing decisions are based on a clear understanding of the teaching methods are used, how the pupils interact with their environment, how teachers address certain types of behaviour, and how the furniture will be used. A thorough risk assessment will assist schools in this process – the Health and Safety Executive (HSE) provides guidance on this.

The location of electrical equipment depends on the length of cables and the availability of sockets for telephones, TV aerials and power. It is essential that the location of the equipment does not increase the risk of danger to equipment or users. The school should ensure that there is a system in place for regular visual checks of plugs, leads and other electrical equipment. Ensure that you have carbon dioxide fire extinguishers positioned near ICT equipment.

Governors need to be aware of these issues to enable them to 'critically question' the school's decisions over health and safety. Further information is published on the ICT Advice website. [**http://www.ictadvice.org.uk/index.php?section=te&rid=151&catcode=as_com_pc_03**]

Useful information

Where can you go for further help regarding ICT?

Your own LEA team, particularly the ICT Adviser, should be your first contact on issues of internet safety and security. Your LEA's Governor Training section may be able to direct you to further local support.

Gridclub

http://www.gridclub.com/

This is a safe online community for children aged 7–11, with over 500 activities aimed at complementing classroom teaching and learning.

Gridclub CyberCafé

http://www.gridclub.com/freearea/internet_safety.html

This section is part of of the Internet Proficiency Scheme, which aims to develop a set of safe and discriminating behaviours for pupils to adopt when using the internet and other technologies.

Health and Safety Executive (HSE)

http://www.hse.gov.uk/pubns/raindex.htm

Guidance on Risk Assessment.

http://www.hse.gov.uk/pubns/iacl97.htm

HSE Workplace Regulations.

Health & Safety in Schools

http://www.governornet.co.uk/cropArticle.cfm?topicAreaId=28&contentId=722&mode=bg

Home Office

http://www.thinkuknow.co.uk/parents

Keep your child safe on the Internet.

Kent LEA Schools Internet Policy 2004/5

http://www.kented.org.uk/ngfl/policy.html

A template to help schools create their own policy.

Kidsmart

http://www.kidsmart.org.uk/

This practical internet safety advice site for schools, agencies and young people is produced by the children's charity Childnet.

Parents Online

http://www.parentsonline.gov.uk/safety/index.html

Created by the DfES to promote home–school links, this aims to increase parents' awareness of how their children can use the internet safely.

Superhighway Safety website

http://safety.ngfl.gov.uk/schools/

This aims to highlight the safety issues regarding new technologies and provides practical information and advice for schools on how to use these technologies safely.

The Schools Buildings Information Centre

http://www.teachernet.gov.uk/schoolbuildings

This document is one of a series, published during Autumn 2004, by Becta to support school governors. Each guide, together with supporting material, will be made available for downloading in the Governor Support area of Becta's website [**http://www.becta.org.uk/leaders/display.cfm?section=13**].

department for
education and skills

Becta
British Educational Communications and Technology Agency

While great care has been taken to ensure that the information in this publication is accurate at the time of publication, we accept no responsibility for any errors or omissions. Where a specific product is referred to in this publication, no recommendation or endorsement of that product by Becta is intended, nor should it be inferred.

Becta is the Government's key partner in the strategic development and delivery of its information and communications technology (ICT) and e-learning strategy for the schools and the learning and skills sectors.

Millburn Hill Road
Science Park
Coventry CV4 7JJ

Tel: 024 7641 6994
Fax: 024 7641 1418

Email: becta@becta.org.uk
URL: http://www.becta.org.uk

12/DD04-05/1007/035/CP/50K