E-safety

Developing whole-school policies to support effective practice

Becta
ICT Advice





The internet, and other digital and information tools, are fast moving technologies with new opportunities emerging daily, along with related issues. This publication offers a snapshot of the situation as it stands in early 2005, but awareness of e-safety issues should be on ongoing process. Any updates or additions to information contained within this publication, therefore, will be posted on the E-safety section on the Becta Schools website [http://www.becta.org.uk/schools/esafety].

Foreword: Developing a whole-school approach to internet safety

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Students with internet access are more confident and have been shown to produce better-researched, more effective and well-presented projects.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A framework of internet safety policies can help to ensure safe and appropriate use. The development and implementation of such strategies should involve all the stakeholders in a child's education from the headteacher and governors to the senior management team and classroom teachers, support staff, parents, and the pupils themselves.

Headteachers, with the support of governors, should take a lead in embedding safe internet practices into the culture of the school, perhaps designating a member of the senior management team with responsibility for internet safety. This member of staff should then act as the central point of contact for all safety issues within the school, ensuring that policies are current and adhered to, instances of breaches and abuse are monitored and reported to the headteacher and governors, and that all staff receive relevant information about emerging issues.

This overall responsibility for internet safety need not necessarily sit with the ICT co-ordinator or network manager, but these staff should work closely with the internet safety co-ordinator to ensure that technological solutions to internet safety support classroom practice. Ultimately the headteacher is responsible for internet safety, in conjunction with the governing body.

It is recommended that, as a minimum, schools have an acceptable use policy in place to protect the interests of both pupils and staff, and that this is at the heart of practice. This should be linked to other mandatory school policies: child protection, health and safety, home–school agreements, and pupil discipline (including the anti-bullying) policy.

Internet safety policies should be regularly monitored and reviewed, and all staff should be aware of the appropriate strategies they should adopt if they encounter problems. Additionally, all school staff have a duty to ensure that pupils using ICT, in any context, are reminded about appropriate behaviour on a regular basis.

This publication is intended to provide guidance for schools on developing appropriate policies and procedures to ensure safe use of the internet by the children and young people in their care. It outlines the risks, suggests a policy framework for schools, and gives an overview of the internet safety responsibilities of all the key stakeholders in a child's education. It also provides practical strategies to follow should problems be encountered.

Please note, this publication does not deal with the health and safety issues relating to ICT use in schools, although further information on this topic is available on the E-safety section on the Becta Schools website [http://www.becta.org.uk/schools/esafety].





Acknowledgements

Becta would like to thank the Internet Safety Group of New Zealand – specifically Liz Butterfield and Claire Balfour, for their help and support in creating this resource, and providing permission for us to use the Netsafe Kit for Schools as a blueprint for this publication [see http://www.netsafe.org.nz].

Becta would also like to thank the following for their support in the writing and producing of this publication:

Barry Phillips
Barry is Strategic eLearning Manager with Sheffield LEA, on secondment from the DfES eLearning Strategy Unit (eLSU). Barry previously worked on DfES policy for the National Learning Network and learndirect.

David Butler
David is chief executive of the National Confederation of Parent Teacher Associations (NCPTA), and a trustee of the e-Learning Foundation.

Fran Stevens
Fran is an educational consultant with a particular interest in the role of school governors. She is the chair of two schools in inner Birmingham, one primary and one secondary, and she also chairs the Birmingham Governor Network.

Harmander Dhanjal
Harmander is an ICT teacher and a head of year at Dixons City Technology College. He is particularly interested in the safe use of ICT, and he has been involved in work to educate parents and pupils through special internet safety evenings.

Judith Pitchforth
Judith has taught in further education for a number of years, teaching mathematics and key skills. She is currently an outreach teacher with responsibility for ICT, working for the Hospital and Home Education Service in Sheffield.

Karl Hopwood
Karl is headteacher of Semley Church of England Voluntary Aided Primary School. He was involved with the initial pilot of the Internet Proficiency Scheme when working as a headteacher in a school in Cumbria, and has recently completed an evaluation of the same scheme in Wiltshire. Karl's school has recently run a series of workshops in which parents and carers work alongside children to explore some of the benefits and dangers of communication technologies.

Detective Sergeant Kevin Borg
Kevin has responsibility for offender management for the West Midlands Police, which includes the co-ordination of the Safer School Partnerships under the Government's Prevent and Deter strategy.

Detective Sergeant Damian Morgan
Damian is a member of the High Tech Crime and Paedophile Unit, and is responsible for the investigation of internet crime within the West Midlands area.

Lynn Barrett
Lynn has worked in school libraries for 20 years, and is now an independent trainer and consultant. She is chair of the School Libraries Group of the Chartered Institute of Library and Information Professionals (CILIP).

Noel Akers
Noel is ICT Systems Manager at Dixons City Technology College and an IT consultant.

Thomas Ng
Thomas is a secondary school ICT consultant from Oxfordshire's ICT advisory team. He project-manages the trial of 'Missing', an internet safety programme, in three secondary schools in Oxfordshire.

Thanks also go to all the individuals and organisations that kindly provided feedback during the draft stages of this publication.

Contents

Foreword: Developing a whole-school approach to internet safety 1

Acknowledgements 2

1 An overview of the risks 4

2 The importance of ensuring a safe ICT learning environment 8
- An infrastructure of whole-school awareness, designated responsibilities, policies and procedures 8
- An effective range of technological tools 10
- A comprehensive internet safety education programme for the whole school community 11

3 Whole-school responsibilities for internet safety 12
- Internet safety co-ordinator 13
- Headteacher 15
- Governing body 16
- Network manager 17
- Subject co-ordinators/heads of department 19
- Heads of year/pastoral team 20
- Classroom teachers and teaching assistants 21
- Special educational needs co-ordinators 24
- Child protection liaison officers 25
- School librarians 26
- Pupils 27
- Other considerations 28

4 Internet safety in the classroom 30

5 Responding to incidents of misuse 32
- Minor incidents 32
- Incidents involving inappropriate materials or activities 33
- Incidents involving illegal materials or activities 34

6 Working with parents and the community 36

7 Sources of further information, advice and support for schools 38

Appendix 1: The legislative perspective 42

Appendix 2: The child protection perspective 44

Appendix 3: Checklists for developing acceptable use policies 46
- School-wide policies and procedures 47
- Communication with parents and carers 47
- Acceptable use guidelines for staff 48
- Acceptable use guidelines for pupils 50
- Internet safety skills development for staff 51
- Internet safety skills development for pupils 51
- Using the technologies safely 52
- School websites 55
- Using images and digital video on school websites 56
- Acceptable use of ICT facilities within the school library 57
- The school as a community resource 57

Appendix 4: Notes on securing and preserving evidence 58
- School premises 58
- Home computers 58
- Flowchart for responding to internet safety incidents in school 59

Appendix 5: Glossary 60




1 An overview of the risks

ICT can offer many positive educational and social benefits to young people, but unfortunately there are some dangers. As in any other area of life, children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. Some of the issues and risks are summarised below.

While many of the issues outlined in this section relate, primarily, to ICT use outside school, it is inevitable that some of the issues, when initiated outside school, will be bought back in and need to be dealt with accordingly by the school. For example, bullying via chat or text messages will impact upon relationships within school; obsessive use of the internet may impact upon the quality of schoolwork; and changes in the personality and general wellbeing of a pupil may indicate that they are involved in inappropriate or illegal behaviours online.

Schools will have technologies in place to restrict inappropriate access, but it must be borne in mind that children will bring an increasingly sophisticated range of handheld devices into school giving them separate access to potentially unsuitable materials. Hence schools' acceptable use policies will also need to consider pupils' own equipment.

Schools therefore have a major responsibility to educate their pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

Young people who have been using the internet excessively, or engaging in risky or illegal behaviours online, may benefit from professional support or counselling to redress the balance of their online and offline life. The school may play a key role in recognising this need, and engaging appropriate help.

Copyright infringement

Copyright law applies on the internet, but is ignored by many young people who download and swap music files, cut and paste homework assignments from others' work, or even purchase whole assignments from online cheat sites without realising the implications and consequences. See the E-safety section on the Becta Schools website for further information on copyright [http://www.becta.org.uk/schools/esafety].

Obsessive use of the internet and ICT

There is the potential for children and young people to become obsessed with the internet and related technologies. Factors such as spending a significant amount of time online, deterioration of the quality of school work, diminished sleep time, or negative impacts upon family relationships, may all be indicators that the internet is taking too high a priority in a young person's life.

Exposure to inappropriate materials

There is a risk that when using the internet, email or chat services, young people may be exposed to inappropriate material. This may be material that is pornographic, hateful or violent in nature, encourages activities that are dangerous or illegal, or is just age-inappropriate or biased. One of the key benefits of the web is that it is open to all, but unfortunately this also means that those with extreme political, racist or sexist views are able to spread their distorted view of the world.

In the case of pornography, there is no doubt that the internet plays host to a large amount of legal and illegal material. Curiosity about pornography is a normal part of sexual development, but young people may be shocked by some of the material online. It is not known what the long-term effects of exposure to such images may be.

Inappropriate or illegal behaviour

Young people may get involved in inappropriate, antisocial or illegal behaviour while using new technologies. Just as in the real world, groups or cliques can form online, and activities that start out as harmless fun, such as voicing an opposing opinion to another member of a chat room, can quickly escalate to something much more serious.

Online bullying is an unfortunate aspect of the use of new technologies, perceived as providing an anonymous method by which bullies can torment their victims at any time of day or night. While a young person may not be in physical danger, they may receive email, chat or text messages that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing.

Some children and young people may become involved in much more serious activities. Possible risks include involvement in identity theft or participation in hate or cult websites, or the buying and selling of stolen goods. The ease of access to online gambling, suicide sites, sites for the sale of weapons, hacking sites, and sites providing recipes for drug or bomb making are also of great concern.

Young people may also become involved in the viewing, possession, making and distribution of indecent and/or child pornographic images. Any concern relating to criminally obscene or criminally racist content can be reported to the Internet Watch Foundation or the police.

Physical danger and sexual abuse

The threat of physical danger is perhaps the most worrying and extreme risk associated with the use of the internet and other technologies.

A criminal minority make use of the internet and related services such as chat rooms to make contact with young people. The intention of these people is to establish and develop relationships with young people with the sole purpose of persuading them into sexual activity. Paedophiles will often target specific individuals, posing as a young person with similar interests and hobbies in order to establish an





online 'friendship'. These relationships may develop over days or weeks, or even months or years, as the paedophile gains the trust and confidence of the young person, perhaps progressing to other forms of contact such as text messaging as a prelude to meeting in person. These techniques are often 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 abuse of the internet and young people.

There is also a risk that while online a young person might provide information that can personally identify them or others, or arrange to meet people they have met online, so posing a risk to their safety or that of their family or friends.

Inappropriate or illegal behaviour by school staff

Unfortunately, school staff have also been found to have been involved in inappropriate or illegal behaviour relating to ICT use. This may include viewing or circulating inappropriate material via email, or much more serious activities such as viewing, possessing, making or distributing indecent and/or child pornographic images. Schools also have a responsibility, therefore, to educate staff as to acceptable behaviours online, and to monitor school networks for evidence of inappropriate activity. Inappropriate activity by a staff member may result in a disciplinary response by the school or authorities. If illegal behaviour by a staff member is suspected, the school has a duty to consult with the police at the earliest opportunity, preserving any potential evidence.

An overview of current legislation which may impact upon the use of the internet and other forms of communication technologies is given in Appendix 1.

Preferences
DateList
Address
Prefs
Default
Done

2 The importance of ensuring a safe ICT learning environment

All schools want to create a safe ICT learning environment, but many are unsure how to begin. Schools are being bombarded with advertising from companies promising that their technological product is the solution to a school's internet safety problems. Such products can be useful, but not when used in isolation. Technological tools are effective only when used in the context of a comprehensive internet safety programme, as outlined below.

Creating a safe ICT learning environment must include:

- an infrastructure of whole-school awareness, designated responsibilities, policies and procedures
- an effective range of technological tools
- a comprehensive internet safety education programme for the whole school community.

The make-up of these components will vary for each school. The needs of a school with a handful of computers are obviously far different from the needs of a complex network for over 1,000 students. Yet the necessity for the three basic components remains the same.

This publication deals mainly with the first of these elements, but reference to the other two are made where appropriate, with pointers to other sources of information.

An infrastructure of whole-school awareness, designated responsibilities, policies and procedures

The first challenge in creating a safe ICT learning environment is to ensure that everyone is aware of the issues and how they impact upon the particular school environment and the pupils within that school. Awareness can be raised, in part, by a comprehensive internet safety education programme for the whole school community. This

programme should be continuous, responding to specific incidents and issues, and providing information about emerging technologies as well as those already embedded within the culture of the school.

The second challenge is in establishing a clear understanding of the responsibilities of all those involved in the education of children and young people with regard to internet safety. Those involved include the headteacher and governing body, senior managers and classroom teachers, child protection and guidance staff, librarians and parents, and the pupils themselves. The responsibilities of these people are discussed in detail in the following sections.

Thirdly, an infrastructure of effective policies and procedures is the backbone to effective practice. Acceptable use policies are documents detailing the ways in which ICT facilities can and cannot be used in school by both pupils and staff, and listing consistent sanctions, procedures and support strategies for dealing with misuse. The policies need to balance the desirability of fully exploiting the vast educational potential of new technologies with providing safeguards against risks and unacceptable material and activities. Reference to internet safety should be included within the school's development plan also.

There are many factors to consider when developing acceptable use policies, and much will depend on local circumstances or the infrastructure of the school. In some instances it may be more appropriate to develop a number of documents as part of the acceptable use policy – for example a management document, a staff use agreement, a pupil/parent use agreement, policies for educating staff and pupils on internet safety issues, and specific procedures for responding to any incidents of misuse. Remember though that it is as important for those involved to have understood and considered the issues as it is to have a written policy document.

An acceptable use policy must be wide-ranging. It must consider: both the fixed and mobile internet; technologies provided by the school (such as PCs, laptops, webcams and digital video equipment); and technologies owned by pupils and staff, but brought onto school premises (such as mobile phones, camera phones, personal digital assistants (PDAs), and portable media players). It should be flexible enough to deal with new and emerging technologies, but should also recognise the important educational and social benefits of such tools.

There are many sample acceptable use policies available, both online and via LEAs, which schools can use as a basis for their own policies. Schools must be aware of the LEA's role regarding internet safety issues. Remember, also, that an effective internet safety policy needs to be tailored to the individual needs of your school. Your policy must consider the particular circumstances of your school, such as race, gender, ethnicity and religious beliefs of pupils and staff, and factors such as the digital divide and access to ICT outside school, which may all have an impact upon the ways in which children and young people use the internet, and the types of potentially risky behaviours they engage in. It is not sufficient to merely take a template and insert your school name – the policy will lack ownership and authority, and may leave your school open to risk.

A person with the designated role of internet safety co-ordinator within the school will assist with creating an acceptable use policy, as discussed in the following section. Additionally, a number of checklists are provided in Appendix 3 giving prompts for issues you may wish to consider when developing your policies. The E-safety section on the Becta Schools website [http://www.becta.org.uk/schools/esafety] provides a range of information to support schools in the development of effective policies and practice.

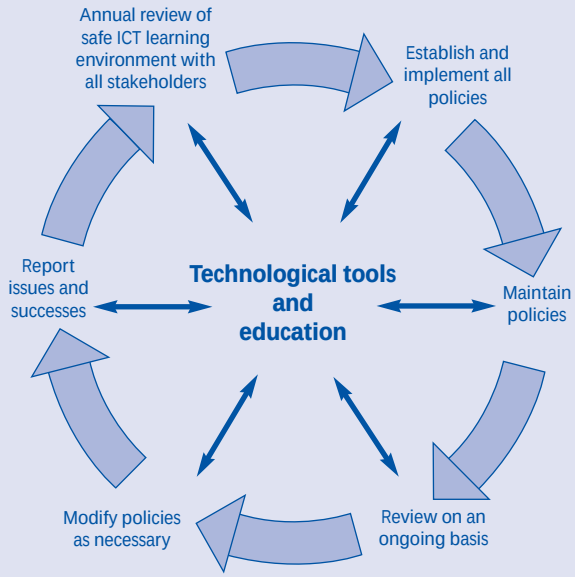
To be truly effective, all school internet safety policies need to be regularly reviewed with all stakeholders (see Section 3) and updated to take account of new and emerging technologies and changes in local circumstances. Ideally, school internet safety policies should be embedded within a cycle of





establishment, maintenance, ongoing review, modification, reporting and annual review, supported by technological solutions wherever possible. By following this process, schools can ensure that they have a rigorous and effective internet safety programme in place.

Creating a safe ICT learning environment



An effective range of technological tools

There are a number of technological tools that schools can employ to safeguard both pupils and the system itself:

- A firewall and virus protection.
- Monitoring systems - to keep track of who downloaded what, when they downloaded it, and using which computer.
- Filtering and content control – to minimise access to inappropriate content via the school network.

There are a range of products to help in these processes and the choice is likely to depend on the school's type, size, in-house technical expertise and budget. Your LEA may be able to offer further guidance on technological tools, or may already provide authority-wide solutions. The Becta accreditation of internet services to education scheme [http://ispsafety.ngfl.gov.uk] enables schools and other educational establishments to make an informed choice of ISP (internet service provider) with a particular emphasis on a safe internet environment.

Becta is putting together a framework of technical, functional and quality-of-service standards that underpin the development of the National Education Network. One of Becta's roles as Network Management Authority is to ensure that these standards are maintained and implemented appropriately. This includes the need to ensure that a safe internet environment is available for schools as an entitlement for all learners and teachers. As a fundamental element of this policy, Becta feels that it is appropriate that all services to schools can demonstrate that they meet the minimum requirements. Becta is therefore working with suppliers to achieve the following objectives:

- Clear definition of the minimum acceptable level of filtering, currently defined within the accreditation scheme.
- Thorough on-site testing and quality assurance of services.
- Agreement of action plans where services do not meet requirements.
- Monitoring action plans until services meet required minimum specifications.

Becta believes that schools should only purchase services from suppliers who meet the minimum requirements. Services that meet the requirements will receive an accreditation mark.

Unfortunately, technological solutions are only one element in the process of creating a safe ICT learning environment: any school which relies solely on technological solutions could be placing themselves, and their pupils and staff, at risk. It is important to reiterate, at this stage, that a school's technological solutions will not be effective against pupils' own equipment.

A comprehensive internet safety education programme for the whole school community

A comprehensive internet safety education programme is an important element in creating a safe ICT learning environment, for both pupils and staff alike. By being informed of the issues and potential risks, users of the internet and related technologies can better take measures to protect themselves and recognise when they might be in danger.

Education is essential in helping children and young people to develop their own parameters of acceptable behaviour when online, and allow them to develop their own strategies for protecting themselves when using ICT in situations where the adult supervision and technological protection offered within the school environment are not available. Children and young people should also be taught to seek help if they experience problems, understanding that they are not accountable, nor should they feel guilty, for the actions of others in which they are unwilling participants. Schools have an important role to play in teaching internet safety. Further information on teaching internet safety in the classroom is given in Section 4.

Through educating school staff, they will be better equipped to support pupils in gaining positive experiences when online, and can help their pupils develop strategies if they should encounter problems. Above all, internet safety education should be a continuing feature of both staff development and pupils' educational development.

Schools also have an important role to play in helping to educate parents and the wider community. For further information, see Section 6.





3 Whole-school responsibilities for internet safety

Internet safety must be a whole-school responsibility. The following sections suggest some action points which each of the key stakeholders in a school may wish to consider.

The headteacher obviously has overall responsibility for the day-to-day administration and management of the school, under the direction of the governing body where appropriate. However, it is advisable for the headteacher to delegate responsibility for internet safety management to a senior manager. For the purposes of this document we will call this role the internet safety co-ordinator.

Internet safety co-ordinator

For the purposes of this publication we have called the senior manager with responsibility for internet safety management the internet safety co-ordinator, but it is up to the individual school what they call this role. What is important, however, is that a title is assigned – unless an actual title accompanies the responsibility there will be less focus on the leadership of one person, and, as a result, potentially a fragmented and therefore less effective school response to associated issues. It is important for the senior manager taking on this role to understand why internet safety is a significant issue for the school – although there are no statutory requirements in this area, all schools have a general duty of care to ensure the safety of their pupils and staff.

The internet safety co-ordinator should have the authority and experience not only to lead a team which establishes and maintains a school-wide internet safety programme, but also to make appropriate responses to policy breaches. Such breaches could involve either employees of the school or pupils, and could be serious enough to risk a pupil's place at the school, or a staff member's employment. If such a serious situation were to occur, the matter would, of course, be handled by the headteacher and/or governing body and LEA as appropriate.

If you suspect a criminal offence has been committed, whether by a pupil or a member of staff, it is essential that the police are consulted at the earliest opportunity. It is crucial to an investigation to secure and preserve evidence as soon as possible – for further information see Section 5, and Appendix 4.

The primary responsibility of the internet safety co-ordinator should be to establish and maintain a safe ICT learning environment within the school. This will obviously involve addressing a range of issues, and taking a number of actions, the details of which will depend upon how advanced the school's internet safety activities are.

The internet safety co-ordinator must be responsible for the following:

- Forming a school internet safety policy team to review and advise on internet safety policies. This may include the ICT co-ordinator, network manager, pastoral care staff, the special educational needs co-ordinator, the child protection liaison officer and the school librarian, although any other member of staff with an interest in this area should also be encouraged to participate. It should also include governor, pupil and parent representatives. The knowledge and relevant perspective of each team member will contribute to the depth and breadth of the school's internet safety policies and programme.
- Due to the sensitivities of some of the issues covered, it may be appropriate to convene a separate internet safety management team consisting of key representatives from the policy team, but without governor, parent or pupil representation. This will provide an opportunity for specific cases or instances of misuse to be discussed and reviewed in confidence.
- Working with the internet safety team and the headteacher to develop, or review, appropriate internet safety policies and procedures.
- Leading on the development of management protocols so that any incidents in which internet safety is breached are responded to in an appropriate and consistent manner, with the appropriate authority to take action as necessary.
- Leading in the creation of a staff professional development programme that addresses both the benefits and risks of communication technologies. This may include written information provided with a staff use agreement, an internet safety manual or handbook for staff, regular presentations at staff meetings, and hands-on training sessions on practical aspects of internet safety. Above all, staff should be made aware that they have professional responsibilities for pupils' safety in this area.





- Leading in the creation of an internet safety education programme for pupils, maintaining an overview of activities across the school, and supporting departments and staff with information and resources as appropriate.
- Developing a parental awareness programme, in consultation with the parent–teacher association, as appropriate.
- Maintaining a log of all incidents relating to internet safety in school.
- Making recommendations for review of policy and technological solutions on the basis of analysis of logs and emerging trends.
- Meeting regularly with the headteacher to discuss internet safety issues and review progress.
- Updating the governing body on current internet safety issues, in conjunction with the headteacher.
- Liaising with outside agencies, which may include the LEA, local schools, city learning centre, or national agencies, as appropriate.

As part of the role, the internet safety co-ordinator should seek to develop a cycle of creation, maintenance, ongoing review, modification and reporting of all internet safety policies and practices (see Section 2). Through this approach, the school can be confident that it has a rigorous and effective internet safety programme in place. This needs to include regular internet safety management team meetings to discuss any reported incidents and issues; regular internet safety policy team meetings to review policy, discuss compliance issues and review how effectively systems are operating; and regular reviews of internet safety education for new staff and new pupils, especially those who arrive during the course of the school year.

In addition, it would be useful to consider emerging trends and issues – data obtained from the monitoring of internet use, technological developments, and any feedback received from staff, pupils and parents. If there have been incidents of misuse or complaints about procedures, these regular meetings will seek to ensure that action is taken as swiftly as possible. The ultimate aim of the internet safety co-ordinator and the internet safety team is to be proactive rather than reactive.

Headteacher

Unless the headteacher takes a special interest in establishing a safe ICT learning environment, it can be very difficult for a school to achieve that goal. This does not mean, however, that the headteacher must personally take on the responsibilities involved; these can be delegated to a senior member of staff in the capacity of internet safety co-ordinator (as outlined above). The headteacher must ensure, however, that the internet safety co-ordinator has the appropriate authority and adequate allocated time to carry out the duties of the role effectively.

Suggested responsibilities for headteachers include:

- taking ultimate responsibility for internet safety issues within the school, while delegating day-to-day responsibility to the internet safety co-ordinator and the school's internet safety team
- ensuring that the internet safety co-ordinator and members of the school's internet safety team are given appropriate time, support and authority to carry out their duties effectively; also, ensuring that developments at local and partnership level are communicated to the internet safety team
- supporting the internet safety co-ordinator in creating an internet safety culture within the school, including speaking to staff and students in support of the programme
- ensuring that the governing body is informed of the issues and the policies
- ensuring that appropriate funding is allocated to support internet safety activities throughout the school, for both the technical infrastructure and Inset training
- promoting internet safety across the curriculum.





Governing body

Governing bodies have statutory responsibilities for child protection and health and safety, and elements of these will include internet safety.

Suggested responsibilities for governing bodies include:

- developing an awareness of the issues and risks of using ICT in schools, alongside the benefits, particularly with regard to the internet and other communications technologies. Consider appointing an e-Governor, that is a governor with specific responsibility for ICT, and ensure that internet safety is included as part of the regular review of child protection and health and safety policies
- developing an understanding of existing school policies, systems and procedures for maintaining a safe ICT learning environment and supporting the headteacher (or designated member of staff) in implementing these, including ensuring access to relevant training for all school staff
- supporting the headteacher (or designated member of staff) in developing an appropriate strategy and plan for dealing with the media should serious incidents occur. In such an instance, it is likely that the chair of the governing body will be approached by the press for comment
- ensuring that appropriate funding is authorised for internet safety solutions, training and other activities as recommended by the headteacher (or designated member of staff), as part of the wider remit of the governing body with regard to school budgets
- promoting internet safety to parents, and providing updates on internet safety policies within the statutory 'security' section of the annual report.

Becta has been commissioned by the DfES to produce a free series of ICT Guides for Governors [http://www.becta.org.uk/leaders/governors].

Network manager

The network manager has an important role to play in establishing and maintaining a safe ICT learning environment for the school, and will be a key member of the school's internet safety team. The person in this post will generally have a high level of technical knowledge and expertise. They will possibly have responsibility for maintaining the school's network and the technological measures for ensuring internet safety. The network manager should work closely with the internet safety co-ordinator to ensure that educational and technological aspects of internet safety support and complement each other.

As part of developing a safe ICT learning environment, there is a requirement for the network manager to receive continuing professional development. At a most basic level, the network manager should be able to carry out regular checks for indications of misuse. In reality, however, a greater level of expertise is required, and so it is important that appropriate training opportunities are available to the person in this post.[1]

If working within a team structure, network managers may wish to carefully consider the processes used for carrying out checks and audits of computer networks – for example, they may wish to consider whether it is appropriate for junior staff to be asked to carry out checks on files of other, possibly more senior, staff members.

If illegal, age-restricted, or legal but seriously inappropriate material is found on the school's network, it is likely that the network manager will be the first to be aware of it.

In the case of indecent material, even if it is just suspected, it is essential that the situation is reported immediately to the police (via the internet safety co-ordinator and/or headteacher). At this stage, in order to prevent potential evidence being compromised, it is important that no technical action is taken by the network manager (or any other staff member). Failure to secure and preserve evidence, if proven, may constitute a criminal offence in itself. For further information, see Section 5 and Appendix 4.

If age-restricted, or legal but seriously inappropriate materials are discovered on the school's network, this is a matter for the school to deal with. Network management procedures should be engaged at the earliest opportunity to ensure that the offending material is removed from the school's network. Technical systems and procedures should be reviewed immediately following the event to prevent such incidents occurring in the future.

If offending materials (or other breaches of acceptable use) can be traced back to individuals, the network manager will need to liaise with pastoral teams (in the case of misuse by pupils) or the internet safety co-ordinator and/or headteacher (in the case of misuse by staff) to ensure that appropriate actions may be taken.

In summary, suggested responsibilities for the network manager include:

- acting as a key member of the school's internet safety team, supporting the internet safety co-ordinator in the development and maintenance of appropriate policies and procedures through technical information and advice
- providing a technical infrastructure to support internet safety practices; this might include:
  - ensuring that appropriate and effective electronic security systems are in place, such as filtering, monitoring and firewall technology, and virus protection supported by regular and thorough monitoring of computer networks

[1] Please note, some commercial companies offer network security and systems audits for schools, and it is up to the individual school whether they choose to use such services. However, if indecent material is suspected on a school network, it is essential that the school consult with the police immediately. Likewise, if indecent material is discovered (or suspected) during a routine system audit by a commercial company, it is essential that it ceases work immediately and reports the situation to the police (informing the school's internet safety co-ordinator and/or headteacher also).





- documenting the location of all internet-accessible computers within the school. Should a serious breach of internet safety occur, detailed, up-to-date, graphical documentation of the school's network and hardware infrastructure can assist with any ensuing investigations (whether internal by the school, or external by the police). Careful consideration should be given to the monitoring of mobile or wireless equipment
- advising on the positioning of internet-enabled computers within the school to allow easy supervision of pupils' work, and hence discourage breaches of acceptable use policies
- ensuring that staff workroom computers are secure
- ensuring that appropriate processes and procedures are in place for responding to the discovery of illegal materials on the school's network, or the suspicion that such materials exist
- ensuring that appropriate processes and procedures are in place for responding to the discovery of inappropriate but legal materials on the school's network.

- reporting network breaches of acceptable use of ICT facilities to the internet safety co-ordinator and other staff members as appropriate
- maintaining an appropriate level of professional conduct in their own internet use both within and outside school.

Subject co-ordinators/heads of department

Subject co-ordinators and heads of department have an important role to play in developing a safe ICT learning environment in schools. As influential leaders of groups of staff, they are key in supporting the internet safety culture within the school.

Suggested responsibilities for subject co-ordinators/heads of department include:

- In consultation with the internet safety co-ordinator, the subject co-ordinator/head of department should develop additional internet safety policies where necessary within the subject area/department.

  A departmental policy should outline the importance of embedding internet safety messages within the context of the curriculum – the Internet Proficiency Scheme (for Key Stage 2), and Signposts to Safety (for Key Stages 3 and 4) provide further information on this. (See pages 21-22 for details).

  The departmental policy should also consider what safety measures are appropriate for a particular situation (for example in the ICT suite or in the classroom), and the specific technologies used within the teaching of the subject.

  Differentiation within a subject area should also be considered – for example, does the department wish to provide access to different online resources for different year groups, for example within citizenship, or dynamic filtering by class or year group?

  A departmental policy should also outline the procedures that staff are expected to follow, especially in relation to the reporting of any incident in which internet use policies have been breached.

- In consultation with the network manager, the subject co-ordinator/head of department should consider how to position departmental computers so that pupils can be suitably supervised. They should ensure that technological security measures are active and appropriate to the work of the department.

- The subject co-ordinator/head of department should ensure a co-ordinated approach across the subject/department to teaching internet safety issues. This includes the responsibility of departmental staff to remind all pupils of the risks, and the pupils' responsibilities, whenever ICT is used.

- The subject co-ordinator/head of department should work with the librarian and others to develop resource-based learning experiences to enable pupils to develop their information literacy skills within the context of the curriculum.

Unfortunately, it is possible that staff themselves can be involved in breaches of school policy, either by neglecting to follow safety procedures with students, or by involvement with inappropriate or illegal material. Obviously it is important that any such issues are immediately reported to the internet safety co-ordinator or the headteacher. If a criminal offence has been committed (in the case of involvement with indecent materials), the police must be consulted also.

General discussion of internet safety matters and departmental compliance issues can take place at regular departmental meetings or during classroom teachers' individual performance appraisals.





Heads of year/pastoral team

The pastoral team plays an important role in the running of a school, and so it is essential that its members are involved in developing a safe ICT learning environment too.

Members of the pastoral team, such as the heads of year or form tutors, have responsibility for the social welfare of pupils within their year group, and, as such, will often be the key point of contact in dealing with incidents of ICT misuse or abuse. The pastoral team will play a key role in imposing sanctions within the whole-school framework of disciplinary measures, and, if more serious incidents occur, must ensure that appropriate reporting and escalation procedures are followed, involving the police and other external agencies as appropriate.

The pastoral team may also be required to act as mediators for ICT-related incidents which occur outside school, such as bullying within chat rooms or the creation of hate websites aimed at individual pupils. In such cases pastoral staff will play a crucial role in working with those pupils involved to ensure that conflicts are resolved, ensuring that the perpetrators are aware of the seriousness of their actions, and that the victims receive the necessary emotional support. It may also be necessary for the pastoral team to work with parents in reinforcing the internet safety and acceptable use messages pupils receive within the home, and possibly with ISPs also to ensure that offensive websites or materials are removed.

It is important that members of the pastoral team do not work in isolation when dealing with issues relating to internet safety – incidents should be logged and reported to the internet safety co-ordinator in line with school policies, and knowledge of emerging issues shared with colleagues to increase awareness and possibly pre-empt future problems.

Suggested responsibilities for heads of year/pastoral team include:

- acting as a key member and first point of contact for the school's internet safety team, supporting the internet safety co-ordinator in the development and maintenance of appropriate policies and procedures relating to pupil welfare
- developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children and young people
- ensuring any instances of ICT misuse, whether accidental or deliberate, are dealt with through the proper channels, reporting to the internet safety co-ordinator in line with school internet safety policies
- ensuring that pupils who experience problems when using the internet are appropriately supported, working with the internet safety co-ordinator, and/or child protection liaison officer as appropriate.

Classroom teachers and teaching assistants

Of major importance in creating a safe ICT learning environment is the internet safety education which occurs in the classroom itself and is initiated by the classroom teacher or teaching assistant. ICT and, specifically, web-based resources are increasingly being used across the curriculum, so it makes sense therefore that guidance on safe use of the internet should be given to pupils wherever and whenever such use occurs.

Internet safety should be embedded within classroom practice. Taking the internet as an example, a comprehensive school internet safety and education programme would include the requirement for subject co-ordinators and heads of departments to develop a policy on how internet access is handled in their particular subject or area. This will depend on such factors as: what type of physical access to the internet is provided in the classrooms and in other sites the classes frequent; the use made of the internet in the learning taking place in the classes; the age of the pupils; and so on. It is then the responsibility of classroom staff to implement such policies.

The central internet safety messages should be as much part of classroom management as safety rules in a science laboratory – safety rules should be clearly posted in the classroom and should be frequently reviewed by the teacher. A good exercise would be to involve pupils in the creation of a set of class internet safety rules. In this way the pupils will feel a greater sense of ownership and, hopefully, display a greater level of understanding of the issues.

A particular challenge is ensuring that classroom staff have the necessary high level of internet safety awareness. It is not uncommon for children and young people to be more ICT literate and internet literate than most of the adults in whose care they are placed. However, children and young people typically underestimate the potential for risk, often lacking the required knowledge, maturity and experience. It is not necessary for classroom staff to be technical experts, so long as they are well informed about the issues and risks involved for young people. The school should ensure the ongoing professional development of all staff in this area. Additionally, the E-safety section on the Becta Schools website [http://www.becta.org.uk/schools/esafety] provides a range of information on the various issues and concerns, which can help teaching staff in developing an understanding of the issues.

Classroom staff are also encouraged to look for other opportunities for teaching internet safety across the curriculum, rather than as a discrete subject, possibly to cover issues that might not typically be encountered during in-school use of ICT. Although internet safety is not explicitly referred to within the National Curriculum at present, there are a number of appropriate areas within the programmes of study that offer opportunities to discuss internet safety issues at both primary and secondary level. Additionally, for secondary pupils, the ICT strand of the Key Stage 3 National Strategy offers further opportunities too.

The following resources can help with teaching internet safety:

- Internet Proficiency Scheme for Key Stage 2 pupils

  The Internet Proficiency Scheme for Key Stage 2 pupils, developed by Becta, QCA and the DfES, aims to develop a set of safe and discriminating behaviours for pupils to adopt when using the internet and other technologies. There is an interactive website, called CyberCafe, and a teachers' pack consisting of teaching activities, pupils' worksheets, advice and information for teachers on internet safety, and certificates to award on completion of the scheme. Although aimed at Key Stage 2, some of the materials may be particularly useful for introducing internet safety topics to pupils in Year 7, or for pupils with special educational needs.

  Information about the scheme, and downloadable files, are available from the CyberCafe website [http://www.gridclub.com/cybercafe/teachers].





- Signposts to safety: Teaching internet safety at Key Stages 3 and 4

  This booklet, developed by Becta, provides signposts for teaching internet safety at Key Stages 3 and 4. It provides background information on the technologies, including their benefits and risks, along with pointers to useful resources and ideas for incorporating internet safety within the curriculum. It specifically maps internet safety issues against the ICT, citizenship and personal, social and health education (PSHE) programmes of study at Key Stages 3 and 4, and against the ICT strand of the Key Stage 3 National Strategy for Years 7, 8 and 9.

  Copies of Signposts to safety are available from Becta [http://www.becta.org.uk/corporate/publications].

Finally, classroom staff are the ones who spend the most time with pupils, and who may have considerable influence on their thinking and attitudes. It may well be that when we ask children and young people to tell a trusted adult if they are worried about their safety, their teacher will be that person. Additionally, classroom staff may notice a change in the behaviour and attitude of a pupil, which they suspect may be as a result of negative experiences on the internet. In both cases, classroom staff should be aware of the appropriate referral process, seeking support from the internet safety co-ordinator, pastoral team and child protection liaison officers as appropriate.

It is interesting to note that the UK Children Go Online survey[2] found that of children who go online weekly, only 8 per cent of children who received pornographic junk mail, and 6 per cent of children who had seen a pornographic website, told their parents or a teacher. This emphasises the importance of teaching staff taking a proactive role in supporting children and young people in their online experiences, both good and bad.

Where a police School Based Officer (SBO) is in post, he or she should be included in the consultation process when there are concerns for a young person suspected of having a negative experience relating to the internet. In the West Midlands, for example, SBOs form part of a Behavioural Education Support Team (BEST) which includes the key agencies concerned with young people. The SBO would assess whether an offence had been committed by or against the young person, and would follow the referral process, which would involve notifying officers with a greater degree of expertise regarding the investigation of internet crime. This type of investigation is treated with much sensitivity, with the young person's interests and wishes being paramount when deciding whether any further action should taken by the police. If the school does not have a designated officer, then the local police station should be contacted.

In summary, suggested responsibilities for classroom staff include:

- developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children and young people
- implementing school and departmental internet safety policies through effective classroom practice
- ensuring any instances of ICT misuse, whether accidental or deliberate, are dealt with through the proper channels, reporting to the internet safety co-ordinator in line with school internet safety policies
- ensuring that they provide the necessary support to pupils who experience problems when using the internet, working with the internet safety co-ordinator, pastoral teams and/or child protection liaison officers as appropriate
- planning classroom use of the internet and ICT facilities to ensure that internet safety is not compromised; for example,

[2] Livingstone, S. and Bober, M. (2004) UK Children Go Online: Surveying the experiences of young people and their parents. Available online [http://www.children-go-online.net].

evaluating websites in advance of classroom use (for example, by bookmarking and caching sites) and ensuring that school filtering levels provide appropriate protection for topics being studied

- embedding teaching of internet safety messages within curriculum areas wherever possible
- maintaining an appropriate level of professional conduct in their own internet use both within and outside school.

Further information on teaching internet safety in the classroom is given in Section 4.





Special educational needs co-ordinators

Special educational needs co-ordinators will have certain responsibilities for internet safety issues in school, above and beyond those of their teaching colleagues.

Primarily, special educational needs co-ordinators should carefully consider the needs of pupils for whom they have responsibility, and whether the general internet safety programme offered by the school is appropriate to the needs of those pupils with special educational needs, or whether additional tailored materials are required.

For example, many pupils with autistic spectrum disorder take messages very literally, and could be persuaded to act upon them. These pupils are likely to need additional advice on safe behaviours and what they should never disclose to others online; they may also need increased supervision. This could include, for example, guidance that before entering into dialogue with anyone new, they should always consult a trusted adult.

Special educational needs co-ordinators may need to work closely with the child protection liaison officer within their school.

Suggested responsibilities for special educational needs co-ordinators include:

- developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children and young people
- developing and maintaining additional policies and internet safety materials, in conjunction with the internet safety co-ordinator and the school's internet safety team, tailored to the special educational needs of pupils
- liaising with parents of pupils with special educational needs to ensure that they are aware of the internet safety issues their children may encounter outside school, and the ways in which they might support them
- co-operating with the child protection liaison officer, as necessary
- liaising with other individuals and organisations, as appropriate, to ensure that those pupils being educated away from school premises still benefit from a safe ICT learning environment.

Additionally, the following sources provide further advice on educational ICT products for learners with special educational needs:

- Becta – Inclusion and Special Educational Needs
  http://schools.becta.org.uk/index.php?section=iu
  Resources and guidance to support an inclusive approach to education.
- Inclusion website http://inclusion.ngfl.gov.uk
  Advice and information on special educational needs and inclusion.
- Communication Aids Project (CAP)
  http://cap.becta.org.uk
  A project designed to help students with significant communication difficulties.
- TechDis http://www.techdis.ac.uk
  The Joint Information Systems Committee (JISC) TechDis service aims to improve provision for disabled staff and students in the further, higher and specialist education sectors through technology.
- RNIB: Technology http://www.rnib.org.uk/technology
  Information on all aspects of access to technology and sight problems.
- AbilityNet http://www.abilitynet.org.uk
  Free information and advice, fact sheets, assessment and training on all areas of assistive technologies.
- SENIT mailing list
  http://lists.becta.org.uk/mailman/listinfo/senit
  The SENIT mailing list is for teachers, advisors and others working within education to share practical advice about how ICT can be used to support pupils with learning difficulties or disabilities.

Child protection liaison officers

Child protection liaison officers, like special educational needs co-ordinators, have special responsibilities for internet safety issues in school. As the first point of contact for any internet safety issue which may compromise the wellbeing of a child or young person (for example, trauma resulting from internet use such as exposure to inappropriate materials or grooming), they must ensure that they are fully aware of the issues which they might encounter, and develop appropriate strategies and policies for dealing with these.

The child protection liaison officer should work closely with the internet safety co-ordinator, and should be a key member of the school's internet safety team. Their presence will ensure that the school is kept aware of the need to educate and support pupils, including those whose misuse of communications technologies has led to a disciplinary response by the school.

The first challenge for the child protection liaison officer is to become more knowledgeable about the issues, especially as they relate to children and young people. Any issues should be considered within the context of other child protection guidance; for example, the Multi-Agency Public Protection Arrangements (MAPPA), the Bichard Inquiry report, new local safeguarding boards and arrangements, and the Children Act 2004 (see Appendix 2 for further details). Technical expertise is not required, but an understanding of the issues is vital. Knowledge should not be confined to those issues which would typically occur within school, but should extend to the full range of risks that children and young people may encounter wherever and whenever they use new technology.

An additional challenge for child protection liaison officers, with the support of the school (and counselling and guidance staff based outside the school), is to proactively educate children and young people about the risks that they may face, and the importance of seeking support if affected by issues, and give them an understanding that they are not to blame for the actions of others while online.

Referral to the child protection liaison officer should be a mandatory element of the disciplinary process for any pupil involved in serious misconduct using the internet and related communication technologies in school. The child protection liaison officer would then take a view on the best course of action in accordance with the nature of the event and the individual child's needs. The child protection liaison officer should also offer facilities for pupils to self-refer, or for teachers to refer if they fear that one of their pupils may be the victim of internet-related abuse, such as bullying by text message or in chat rooms.

The child protection liaison officer should also form strong relationships with counselling and guidance staff operating outside the school (for example, educational psychologists operating at LEA level) on all matters relating to internet safety and the wellbeing of pupils.

In summary, suggested responsibilities for child protection liaison officers include:

- seeking professional development on the safety issues relating to use of the internet and related technologies, and how these relate to children and young people, refreshing this knowledge on a regular basis
- acting as a key member of the school's internet safety team, liaising with the internet safety co-ordinator on specific incidents of misuse, and providing follow-up counselling and support to both victims and perpetrators as appropriate
- taking a proactive role in the internet safety education of pupils
- developing systems and procedures for supporting and/or referring on pupils referred to them as a result of breaches of internet safety within schools
- developing systems and procedures for pupils who self-refer, and those pupils identified as suspected 'victims' by teaching staff
- developing relationships with colleagues at LEA level (including counsellors and guidance staff) and other organisations that can provide advice, referrals or resources on issues relating to child protection on the internet. In serious cases this might include specialist counselling for addiction to online games, or sexual offender treatment programmes, for example.





School librarians

The library has traditionally played a very special role in the life of a school. Not only is it an information and resource centre for both staff and students, but information literacy skills, along with an enjoyment of reading, are fostered by school librarians. The library offers facilities for research, homework, personal studies and, for some pupils, offers a place of sanctuary. Above all, the school library can offer important ICT facilities to pupils who do not have resources at home, so giving them the same opportunities as other pupils.

However, several factors can make the creation of a safe ICT learning environment more complex and challenging in a school library than in the classroom or ICT suite. Good library design can ensure that internet-accessible computers can be positioned in view of the librarian's workstation, but the librarian is often involved in activities elsewhere. In a large school, the librarian will not necessarily know the identity of all pupils, which may encourage some pupils to feel that they can bend the rules slightly with regards to acceptable use. When a teacher brings a class into the library, the supervision and monitoring is the responsibility of that teacher; however, the supervision of pupils who use the library individually during class time, and the large numbers present at other times of the day, can present very real challenges for the school librarian.

To counter these challenges, it is recommended that a separate or additional acceptable use policy relating to ICT use in the school library is developed. This might include procedures for using ICT equipment in the library (such as a booking system), guidelines for staff on class use of the library facilities and individual use by pupils in class time, and any internet use policies specific to library circumstances. A checklist for developing an acceptable use policy for a library is given in Appendix 3.

Suggested responsibilities for the school librarian include:

- acting as a key member of the school's internet safety team
- developing an acceptable use policy for the library, as appropriate to the needs of the school and the library
- providing specialist input to both the internet safety co-ordinator and the network manager on filtering issues, with particular reference to the age and research activities of pupils at the school (filtering tools can sometimes create barriers to older students engaged in legitimate research)
- advising on issues relating to information-handling skills (for example, effective search skills) and information literacy as part of pupils' independent learning development, and working with teaching staff to ensure that this is also embedded within the context of the curriculum
- seeking professional development opportunities for developing and maintaining knowledge on internet safety issues; professional associations, such as the Chartered Institute of Library and Information Professionals (CILIP) [http://www.cilip.org.uk] and the School Library Association [http://www.sla.org.uk] may be able to assist with information, training and resources.

Pupils

The responsibilities of the pupils themselves in creating a safe ICT learning environment should not be underestimated.

Pupils should be encouraged to contribute to the creation of school policies, with pupil representation on the school's internet safety policy team and involvement in developing classroom rules and internet safety resources. Through this approach, pupils will develop a greater understanding of the issues involved, and will feel more ownership of and accountability for the policies.

The ultimate aim is for pupils to take responsibility for their own actions when using the internet and other communications technologies, with each pupil developing a set of safe and discriminating behaviours to guide their own internet use. Pupils should develop confidence in their own abilities, but should also recognise when it is appropriate to seek help and advice, and know where such help can be found. Pupils should also take a responsibility for talking to their parents or carers about internet safety issues, working with them to develop a set of rules for safe internet use in the home.

Specific responsibilities for pupils might include:

- contributing to school internet safety and acceptable use policies through involvement in the school's internet safety policy team
- upholding school policies relating to acceptable use of the internet and other communications technologies
- developing their own set of safe and discriminating behaviours to guide them whenever they are online
- reporting any incidents of ICT misuse within school to a member of the teaching staff
- seeking help or advice from a teacher or trusted adult if they experience problems when online, or if they receive any content or contact which makes them feel uncomfortable in any way
- communicating with their parents or carers about internet safety issues, and upholding any rules for safe internet use in the home.





Other considerations

Children educated outside mainstream school

The internet safety requirements of children educated outside mainstream school must also be considered. These may be pupils who are educated away from the main school site for medical or related reasons, those who are anxious and withdrawn, those who have been excluded from mainstream education, and, increasingly, those being educated at colleges or in work-based learning as part of the developing 14-19 agenda. Many of these young people may be out of school on a temporary basis only.

This group of pupils may be particularly vulnerable and it is especially important that they are taught to develop their own parameters of acceptable behaviour when online, and are able to protect themselves when using ICT without adult supervision. For many of these young people use of the internet will be an essential tool in their education, and, for most students, the positive aspects of it will far outweigh the possible dangers.

Some of these children may be taught in LEA establishments, local libraries, city learning centres or other places in the community that may have their own security systems in place, and it is important that the teacher is aware of what these systems are. For pupils taught only in the home environment it is possible that there may be little or no security or technological protection available, and it is especially important that the young people are educated to be able to deal with this and to seek help from a responsible adult, should they experience problems.

In hospitals where ward-based access to the internet is available to assist children and young people to continue with their academic work, it is important to ensure that, as far as possible, the standards of security and technological protection, and the standards to which pupils are expected to adhere within school, are maintained. If specific technologies are used, it is essential that children and young people are aware of any specific issues relating to them. If using webcams, for example, pupils should be aware of the risks of Trojan horses. Put simply, a Trojan horse is a program than infects your computer and allows a hacker to run hidden tasks without your knowledge. Trojan horses are typically spread via executable files as email attachments, or may be buried within legitimate files making it very difficult to detect their presence. Once present, Trojan horses allow hackers to read or modify files on your hard disk, log anything you type using your keyboard, or even control your webcam, switching it on and off, and therefore viewing you, without your knowledge. Good anti-virus software may help to protect against Trojan horses, and there are many anti-Trojan packages also available. Young people should also be aware of the need for appropriate dress when using webcams.

LEAs

LEAs, while obviously not taking a specific role within the management of any individual school, still have an important role to play in developing a safe ICT learning environment.

The LEA may be able to assist on several levels:

- The LEA may have developed an authority-wide policy with regard to internet use and internet safety within schools, which may include policy templates which the school can amend for its own use. Remember, however, that an effective internet safety policy needs to be tailored to the individual needs of your school, and is as much about an understanding and consideration of the issues as having a written policy document. It is not sufficient to merely take a template and insert your school name – the policy will lack ownership, authority and authenticity.
- The LEA may have implemented authority-wide access and/or provisions for the technological aspects of internet safety, possibly providing a managed service giving filtering, blocking, monitoring and firewall functionality. The LEA may be also able to offer training to key staff members in this area, helpdesk facilities for support with specific technical issues, or possibly a forum to discuss these issues.

- In the case of internet misuse by staff, the LEA may be a useful point of contact for advice and guidance on implementing disciplinary procedures.
- In the case of internet misuse by pupils, the LEA may be a key point of contact for engaging additional support services (for example, counsellors and educational psychologists).
- The LEA may be able to offer a model media plan should incidents of serious misuse occur.





4 Internet safety in the classroom

Education on internet safety issues is essential – although there are many powerful benefits to the use of the internet and communications technologies, this new environment can present very real and serious risks for the uninformed, the unwary and the unwise. Children and young people, whom society has a duty to protect, may be the ones most at risk.

It is important that teachers, parents and carers do not confuse skilful use of new technologies with an ability to perceive and avoid risk – internet and ICT literacy is unfortunately not synonymous with internet and ICT safety.

Schools have a responsibility to educate young people and provide a safe learning environment. Increasingly, ICT is used as an integral part of teaching and learning, and evidence shows that it can have many important benefits. Schools, therefore, must also play a special role in educating children and young people about safe use of the internet and related technologies. Classroom teachers and teaching assistants will be instrumental in this process.

Careful consideration should be given to where and when internet safety education takes place. While discrete lessons are useful, internet safety concepts should be embedded within the curriculum wherever possible, while safety messages should be reinforced every time pupils use the internet and related technologies. Classroom staff should work together with their subject co-ordinators or heads of department, the internet safety co-ordinator and the librarian, to ensure that a comprehensive, consistent and continuing programme of internet safety education takes place across subjects, year groups and throughout the school.

There is also the need to consider the level of experience of the pupil, rather than just their age, when introducing internet safety topics. The Internet Proficiency Scheme (see below and page 21) suggests a framework for profiling pupils. In this model, three groups of pupils were identified. These groups were based on the level of ICT experience of pupils, their prior exposure to internet safety advice, and the degree to which they engaged in potentially risky online behaviour. It was found that children generally fell into one of three broad categories:

- Group A: Those with low levels of experience of the internet, low levels of prior exposure to internet safety advice, and poor ICT skills. This group will generally need guided learning, requiring the teacher to work more closely with the pupils, and provide appropriate prompts.
- Group B: Those with moderate levels of experience of using the internet, moderate levels of prior exposure to internet safety advice, and moderate ICT skills. This group can be considered as having a moderate skill and knowledge base. This group will typically benefit from resource-based learning to help them develop information literacy skills and independent learning skills.
- Group C: Children with high levels of experience using the internet, high levels of prior exposure to internet safety advice, and good ICT skills. These children generally have a good skills and knowledge base, and need to develop their abilities to reflect and apply their thinking to new situations. Note: knowledge of internet safety advice is no guarantee that children will not engage in risky online behaviour – children in this group need just as much safety education as the other groups, as this group is more likely to take risks.

Although initially devised for Key Stage 2 pupils, this model could usefully be adapted for use throughout the school. Remember also, factors such as race, gender and ethnicity may have a bearing on the model of internet safety education used within your school.

There are many resources available to help teachers in providing internet safety education in the classroom. Two key items from Becta, as already discussed, are the Internet Proficiency Scheme for Key Stage 2 pupils and Signposts to safety: Teaching internet safety at Key Stages 3 and 4. (See pages 21-22 for further information and ordering details).

Further information on the role of classroom teachers and teaching assistants is given in Section 3.





5 Responding to incidents of misuse

Even with all the policies and technological solutions in place, there may still be occasions when misuse of the internet and related technologies occur. Schools must ensure that they have appropriate strategies in place for responding to such instances.

Senior managers in schools are required to respond to a wide variety of incidents on a daily basis. Most of these incidents are minor, but some are more serious. The majority involve students, but on occasion it may be a teaching or non-teaching member of staff whose conduct is in question. Schools generally work from procedures which are based on school policy and established practice to deal with such incidents. However, responding appropriately to a breach of internet safety can cause some uncertainty, sometimes over what the nature of the offence may be, or even because of a lack of understanding of the potential seriousness of incidents involving ICT.

This section provides some examples of ICT-related incidents which schools might encounter, and suggests some strategies for dealing with them.

Minor incidents

Minor incidents of misuse by pupils might include:

- copying information into assignments and failing to acknowledge the source (plagiarism and copyright infringement)
- downloading materials or images not relevant to their studies, in direct breach of the school's acceptable use policy
- misconduct associated with student logins, such as using someone else's password
- incidents involving pupils using their own technology in school, such as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorised taking of images with a mobile phone camera, still or moving.

Schools will have their own rules about particular technologies, and, in theory, many of these issues should have been covered within the school's acceptable use policy. In all but the most minor of cases it would be wise for the pupil to be issued with a warning, and the incident documented. If the behaviour is repeated, or the misconduct escalates, it can then be responded to more seriously if the school has evidence of previous events. Any incident of racially motivated abuse via technology needs to be linked in with the monitoring of racial incidents in the school.

The internet safety co-ordinator should monitor minor incidents to identify trends in pupils' behaviour, and should react proactively to any emerging issues. This might include raising awareness on a particular internet safety topic at a school assembly or offering staff additional training. It is also wise to periodically review the school's internet safety policies, and, in particular, acceptable use policies, to see if they should be modified in any way.

Incidents involving inappropriate materials or activities

While not illegal, there will be some material that is just not appropriate within the school environment, and, in the case of staff, not in keeping with the professional standards or code of ethics of those who work with children and young people. Examples might include soft-core pornography, hate material, drug or bomb-making recipes, or material that others may find offensive such as sexist or racist jokes, cartoons, or material which is used in low-level harassment.

Specific breaches of policy and rules might include deliberately accessing, printing, showing or transmitting inappropriate (or age-restricted) material within the school's network. Even if such material was not deliberately accessed by the pupil, but not reported to a teacher, and was subsequently shown to other students, this should also merit a disciplinary response.

Other incidents of more serious misuse by pupils might include cheating in an examination or plagiarism in coursework, which, aside from infringing school assessment policies, may have legal implications (for example, they may breach copyright law). Hacking, virus attack, chronic truancy (as a result of obsessive or excessive use of the internet and related technologies) and online gambling are all serious concerns for schools, and require a disciplinary response.

Age-restricted material is potentially more serious. Publications are classified to provide information and protect people from viewing material that might be inappropriate or damaging to their moral and physical wellbeing. It is therefore illegal to show, give or sell restricted materials to a person under a certain age. Blatant, intentional exhibiting of age-restricted materials to pupils under the specified age is a serious breach of internet safety and should invoke a strong disciplinary response from the school.

Any incident involving a member of staff is a serious, and often complex, matter. There may be implications for the safety of pupils, fellow employees and the learning environment, and for the reputation of the school. Schools should, in the first instance, ensure that they have an acceptable use policy for staff and that policies and procedures are in place should incidents occur.

Harassment of another person using ICT, or breaching their right to privacy, poses a serious threat to their physical and emotional safety, and again may have legal consequences.

More serious incidents relating to internet safety in schools should be reported to the internet safety co-ordinator immediately. The internet safety co-ordinator must document the incident and decide on an appropriate course of action, which may include involving the headteacher and external agencies. It may also be necessary to involve child protection staff to provide follow-up counselling and support to both the victims and perpetrators. The internet safety co-ordinator should review internet safety policies as soon as possible after the incident in an attempt to prevent such an incident recurring, debriefing relevant staff accordingly, and providing school-wide training as appropriate.





Incidents that involve inappropriate but legal material should be dealt with by the school via the usual disciplinary system; unless a criminal offence has been committed, it is not normally necessary to involve the police. Depending on the nature of the incident there may be breaches of other school policies, such as the anti-bullying policy, which may also warrant review. Disciplinary action may range from a warning to dismissal of a staff member or suspension of a pupil. As in all disciplinary instances of this seriousness, a school must be careful to follow disciplinary protocols, ensuring that proper documentation and recording of information occurs, and that appropriate counselling and support are given, and ensuring that parents and carers of the pupil involved are kept fully informed of the matter.

If police involvement is necessary, it is advisable for the headteacher to seek legal advice, via their LEA, as soon as possible.

Any serious incidents could become the subject of media attention. Schools should ensure that they have an appropriate strategy in place for dealing with media requests, and ensure that ongoing investigations and the continuing safety of the school are not compromised by media coverage.

Incidents involving illegal materials or activities

In the school context, very serious incidents tend to involve illegal materials (particularly the viewing, possession, making and distribution of indecent images of children) or serious stalking or harassment facilitated by communication technologies. Such criminal offences may be committed by staff and pupils alike.

Indecent images of children are defined under Section 7 of the Protection of Children Act 1978 (as amended by Section 84 of the Criminal Justice and Public Order Act 1994). References to indecent photographs under the Act include data stored on a computer disk or by other electronic means that is capable of conversion into a photograph.

The Protection from Harassment Act 1997 is intended to prevent 'stalking' and other similar unsocial conduct. It states that a person must not pursue a course of conduct which amounts to harassment of another, and which he/she knows, or ought to know, amounts to harassment of the other. Although the term is deliberately not defined in the Act, words such as 'alarm', 'distress' or 'torment' fit the term most accurately, and some adverse impact on the victim is required. To constitute a 'course of conduct', harassment must take place on a minimum of two occasions.

Discovery of indecent material within the school's network is a very serious situation, and must always be reported to the police. It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off. It may be necessary to shut down the whole network, but do not do this unless instructed by the police. Ensure that everyone is kept away and that nothing is touched. Under no circumstances should the internet safety co-ordinator, network manager or headteacher attempt to conduct an investigation of their own, or bring in an outside 'expert' to do so, as this may compromise the evidence if a legal case were to result. In some cases this may constitute a criminal offence in itself.

Further notes on securing and preserving evidence are contained in Appendix 4.

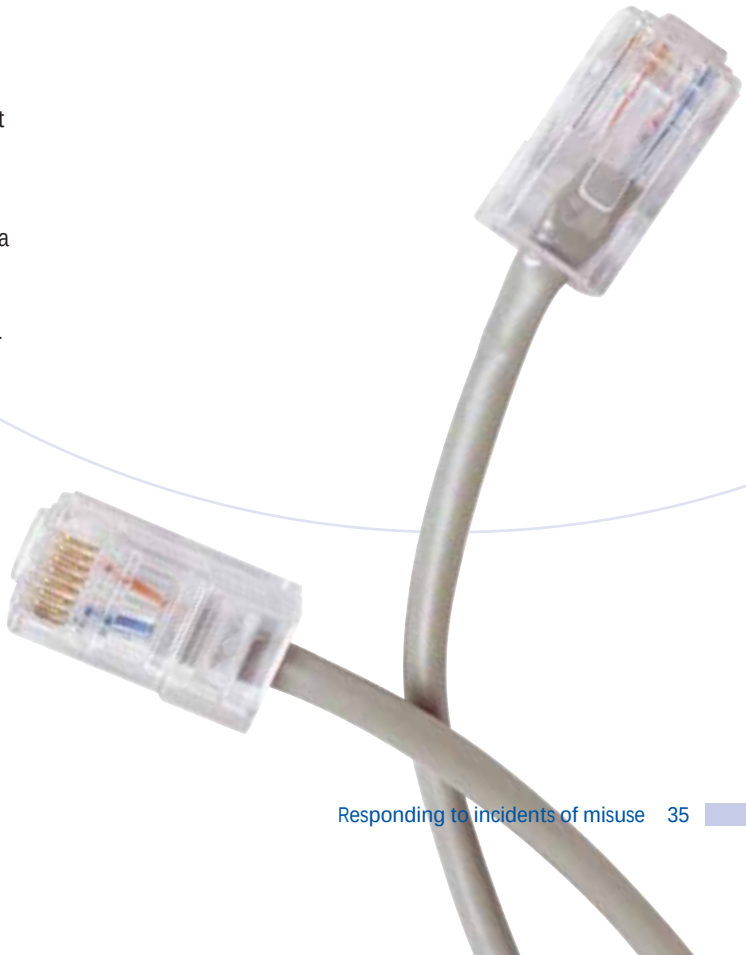
In cases of pupil or staff involvement with indecent materials, it would be sensible for the school to seek legal advice as soon as possible, particularly with regard to the disciplinary actions that are acceptable while the police carry out their investigations. Schools should also be prepared for media contact, and have strategies in place for dealing with this.

In the event of a very serious incident occurring within school, it is essential that a review of all internet safety policies and procedures is conducted as soon as possible. The headteacher would have ultimate responsibility for the review process, but would probably delegate this to the internet safety co-ordinator and the school's internet safety team.

The three key components of a safe ICT learning environment (the infrastructure of whole-school awareness, designated responsibilities, policies and procedures; the effective range of technological tools; and a comprehensive internet safety education programme) should also be reviewed, ensuring that:

- comprehensive debriefing occurs after the incident to maximise what can be learnt
- the network manager has the professional skills to carry out regular safety checks, and knows the correct protocols to follow if illegal material is suspected or encountered
- all school staff understand the circumstances under which a forensic audit of computers should be carried out, and by whom, and the appropriate strategies to adopt to ensure that evidence is secured and preserved (see Appendix 4 for further information)
- the school's internet safety team (both policy and management) contains staff with all the relevant expertise, and that the appropriate time and authority is allocated to the team to allow them to carry out their duties effectively.

Further information on illegal content – including when, where and how to report it – can also be found on the Internet Watch Foundation website [http://www.iwf.org.uk].







6 Working with parents and the community

Parents and carers also have a key role to play in creating a safe ICT learning environment and culture, through promoting internet safety at home and hence reinforcing the messages taught in school.

When talking to parents about home ICT usage, it is important to note that there will be additional equipment found in the home, not normally associated with school use. For example, many games consoles also offer internet connectivity, so parents also need to be aware of the potential hazards related to these items.

Schools should support parents in gaining an appreciation of internet safety, possibly by running workshops or training sessions informing them of the issues, sharing information on internet safety policies and procedures within school, and suggesting practical strategies which parents may wish to adopt in the home.

The school's parent–teacher association may be able to assist with the organisation or promotion of an internet safety event. Likewise, parents or carers with a high level of computer literacy and an understanding of internet safety issues may be willing to assist, while local business owners or ICT professionals may also be able to offer some expertise.

Children's charities NCH and Childnet International offer parental support services to schools wishing to host events or obtain leaflets:

- NCH
  Web: http://www.nch.org.uk/itok
  Email: youthteam@nch.org.uk
  Tel: 0121 321 5190
- Kidsmart
  Web: http://www.kidsmart.org.uk/teachers/helpparents.aspx
  Email: helen@childnet-int.org
  Tel: 020 7639 6967

Additionally, the Home Office, as part of the think U know campaign, provides guidance on keeping your child safe on the internet. A useful booklet is available to download online [http://www.thinkuknow.co.uk/parents.htm]. The Parentscentre website also has detailed safety information and links to websites for parents [http://www.parentscentre.gov.uk]. The Get Safe Online website gives expert advice on how to protect against threats on the internet [http://www.getsafeonline.org].

Other useful resources and points of contact are contained in Section 7.

A challenge for schools when working with parents and carers is that many adults may feel discouraged by their own lack of ICT skills and the ease with which even their youngest children get to grips with communication technologies. At the same time, however, parents and carers may be worried about their children's safety and wellbeing when using the internet and related technologies. With education and support, parents and carers can become confident users of the technologies themselves, and can more effectively guide and support their children's exploration of the internet. However, even very competent and confident adult users of ICT can be unaware of the risks their children may encounter when online; it is not always just beginners who benefit from education and support.

Case study: Promoting internet safety to parents

In the wake of a number of high-profile incidents, and in response to growing public concern about internet safety, Sheffield West City Learning Centre instigated an awareness-raising programme for parents at its partnership schools during 2004.

Aware that the very real fears of parents must be eased, but that a simple evangelical approach would have limited credibility and impact, the city learning centre worked with LEA e-learning officers to devise a pilot programme which involved South Yorkshire Police Sexual Offences and Child Abuse Unit and GridClub [http://www.gridclub.com], a safe online site for 7- to 11-year-olds. The city learning centre then took a mobile classroom, containing an interactive whiteboard and laptops, to four primary schools for early evening sessions. Each session involved short presentations from the participating organisations, questions from the floor and opportunities for parents to have hands-on experience of the internet and, in particular, GridClub. Eighty-six parents attended the first four events, and feedback has been overwhelmingly positive.

Attendance by senior representatives from the council, including the Council Cabinet Member for Inclusive Education and the Lord Mayor, ensured media coverage and raised the profile of the programme. It also demonstrated the council's commitment to promoting the safe use of ICT in its schools through working with parents to alleviate their concerns, and educating and safeguarding their children.

Building on this success, all Sheffield's city learning centres are now developing a city-wide programme to be rolled out in the 2004-05 school year. It is not realistic to take the programme to all 160 primary schools, but the aim is to offer all parents an opportunity to attend a session, whether it is led by the city learning centre or hosted by individual schools. The city learning centres are also planning to make digital video and other resources available to parents via the e-sy.info virtual learning environment before the end of the 2005 school year.

7 Sources of further information, advice and support for schools

Becta Accreditation of Internet Services to Education scheme
http://ispsafety.ngfl.gov.uk

The Becta Accreditation of Internet Services to Education scheme enables schools and other educational establishments to make an informed choice of ISP. The standards of assessment have been developed in consultation with partners in education and industry to ensure reliable and relevant information is provided. The accreditation process makes a technical assessment of filtering services provided by ISPs for factors such as browsing of web-based content, email filtering, blocking and filtering of newsgroups and chat services, and virus alerting. Assessments of service options such as customised filtering for different user groups are also made.

Bullying online
http://www.bullying.co.uk

Bullying Online is an online help and advice service combating all forms of bullying. Recognising that many young people that have lost friends through being bullied in the real world may turn to the internet to make new friends, the 'Staying safe in cyberspace' section gives tips for staying safe in chat rooms. There is also a section on mobile phone bullying, giving tips on how to protect yourself, and information on how the law can help. The site provides information for pupils, teachers and parents.

Childnet International
http://www.childnet-int.org/safety/parents.aspx

Childnet International provides a range of resources to support schools in sharing internet safety information with parents and carers.

Becta Schools Site
http://schools.becta.org.uk/

The Becta Schools Site offers a number of online communities and forums. Each online community focuses on a different aspect of the use of ICT in education, such as a particular technology or classroom practice, or planning and management issues such as internet safety. The communities are also a good place to share advice, get feedback on ideas and talk to colleagues with experience of similar roles and situations. Joining an online community can also help you stay informed (and let you inform others) about events, resources or training opportunities. Participation takes place via email groups which are free to join. All you need is an email address that you can access and check for messages regularly.

To join a group, just visit the Becta Schools site and click on the 'Communities' link to see a list of current categories. Once you have found a community you would like to join, click the 'Register' link to start making contributions. You can subscribe to as many groups as you want. Many forums also provide searchable archives of discussions.

Internet Watch Foundation
http://www.iwf.org.uk

The Internet Watch Foundation (IWF) was formed in 1996 following an agreement between the Government, police and the ISP industry that a partnership approach was needed to tackle the distribution of child abuse images (often referred to as child pornography) online. The IWF operates the only authorised hotline in the UK for the public to report their inadvertent exposure to illegal content on the internet, specifically child abuse images hosted anywhere in the world, and obscene and racist content hosted in the UK. The IWF also provides a 'notice and take down' service to ISPs in the UK so they can remove potentially illegal content from their servers. It works closely with law enforcement agencies at home and abroad to help them trace offenders.

LEAs

Your LEA will undoubtedly be a key resource in helping you to develop a whole-school approach to internet safety. You may find that your LEA has already developed a range of acceptable use policies which can be tailored to the needs of your school, that it offers authority-wide filtering and monitoring solutions, or has defined a set of procedures for auditing networks and responding to serious incidents of misuse.

National Confederation of Parent Teacher Associations (NCPTA)
http://www.ncpta.org.uk

The NCPTA exists to support effective partnerships between parents and teachers which foster learning opportunities both in and out of school. It provides a series of information sheets including one on the internet and its benefits.

NCH IT OK
http://www.nch.org.uk/itok

NCH IT OK provides information for schools and parents on safe internet use.

Parentscentre
http://www.parentscentre.gov.uk

Parentscentre offers support, information and advice on children's learning and the education system, including use of the internet.

Regional police forces and local community police officers

Many regional police forces run internet safety programmes and may be able to provide specialist training and advice in schools. As an example, in the West Midlands, School Based Officers (SBOs) within 21 schools and Young Persons Officers have received training to present internet safety training packages.

If an SBO is not present within your school, it may be wise to discuss issues relating to internet safety in school with your local community police officer, who should be a key point of contact should serious incidents involving illegal material or serious threats to the safety or wellbeing of an individual occur within school.





E-safety on the Becta Schools website
http://www.becta.org.uk/schools/esafety

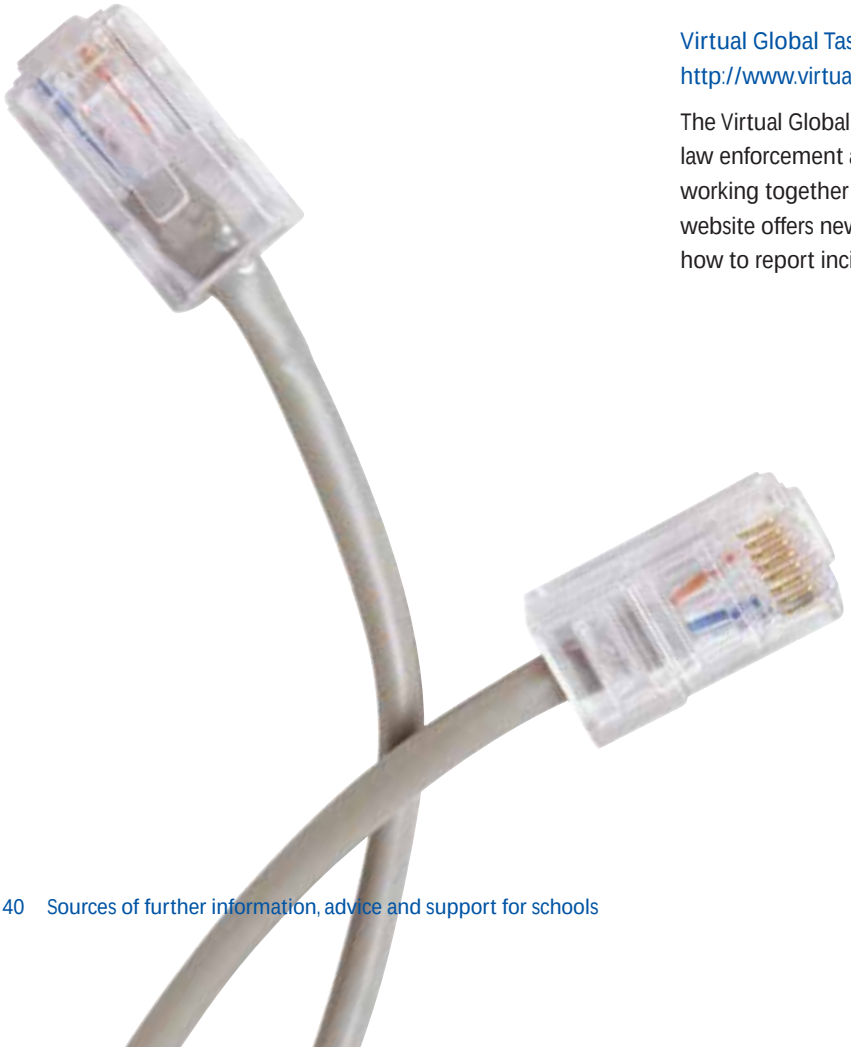
The E-safety section of the Becta schools website aims to highlight the safety issues relating to new technologies and provide practical information and advice for schools on how to use these technologies safely. The site is regularly updated with information on emerging technologies and issues and there are a number of examples of good practice in areas such as email, chat rooms and acceptable use policies.

Case studies of effective practice in promoting the safe use of ICT in education are welcomed, and may be sent by email [internetprof@becta.org.uk].

Any updates or additions to information contained within this publication will also be posted on the E-safety section of the Becta Schools website.

Virtual Global Taskforce
http://www.virtualglobaltaskforce.org

The Virtual Global Taskforce (VGT) is an international alliance of law enforcement agencies created in 2003. These agencies are working together to make the internet a safer place and the website offers news, advice and support, and information on how to report incidents of abuse.







Appendix 1: The legislative perspective

Internet use and abuse is governed by many civil or criminal laws in the UK. While this list is not exhaustive, some of the key provisions are summarised below:

- Computer Misuse Act 1990
  (including hacking, denial of service attacks)
  http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
- Copyright, Designs and Patents Act 1988
  (including copyright theft)
  http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm
- Crime and Disorder Act 1998
  http://www.opsi.gov.uk/acts/acts1998/19980037.htm
- Data Protection Act 1998
  http://www.opsi.gov.uk/acts/acts1998/19980029.htm
- Privacy and Electronic Communications (EC Directive) Regulations 2003
  (including spam)
  http://www.opsi.gov.uk/si/si2003/20032426.htm
- Protection from Harassment Act 1997
  (including harassment, bullying, and cyberstalking)
  http://www.opsi.gov.uk/acts/acts1997/1997040.htm
- Protection of Children Act 1978, as amended by Section 84 of the Criminal Justice and Public Order Act 1994
  (including indecent images of children)
  http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm
- Malicious Communications Act 1988
  (including harassment, bullying, and cyberstalking)
  http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm

- Sexual Offences Act 2003
  (including grooming)
  http://www.opsi.gov.uk/acts/acts2003/20030042.htm
- The Obscene Publications Act 1959 and 1964
  (including illegal material on, or transmitted via, the web and electronic communications)
  - not available online
- The Telecommunications Act 1984
  (including illegal material on, or transmitted via, the web and electronic communications)
  - not available online

Many regional police forces have developed their own educational programmes, and are working with schools to promote internet safety messages, while the National Hi-Tech Crime Unit (NHCTU) [http://www.nhtcu.org] has also been created to combat hi-tech crime within, or which impacts upon, the United Kingdom.





Appendix 2: The child protection perspective

Internet safety within schools needs to be considered within the wider context of child protection issues. While this list is not exhaustive, some of the key child protection provisions are summarised below:

- Bichard Inquiry report
  http://www.bichardinquiry.org.uk
- Children Act 1989
  http://www.opsi.gov.uk/acts/acts1989/Ukpga_19890041_en_1.htm
- Children Act 2004
  http://www.opsi.gov.uk/acts/acts2004/20040031.htm
- Children's National Service Framework
  http://www.dh.gov.uk/PolicyAndGuidance/HealthAndSocialCareTopics/ChildrenServices
- Circular 10/95 – Protecting Children from Abuse: the Role of the Education Service
  http://www.dfes.gov.uk/publications/guidanceonthelaw/10_95/summary.htm
- Education Act 2002
  http://www.opsi.gov.uk/acts/acts2002/20020032.htm
- Every Child Matters
  http://www.everychildmatters.gov.uk
- Guide to the Law for School Governors 2004, Chapter 15 – Health, safety and welfare
  http://www.governornet.co.uk/gttl
- Multi-Agency Public Protection Arrangements (MAPPA)
  http://www.probation.homeoffice.gov.uk/output/page4.asp

- Safeguarding Children in Education
  http://publications.teachernet.gov.uk/eOrderingDownload/DfES-0027-2004.pdf
- Sexual Offences Act 2003
  http://www.opsi.gov.uk/acts/acts2003/20030042.htm





Appendix 3: Checklists for developing acceptable use policies

Checklists provided in this appendix are:

- School-wide policies and procedures
- Communication with parents and carers
- Acceptable use guidelines for staff
- Acceptable use guidelines for pupils
- Internet safety skills development for staff
- Internet safety skills development for pupils
- Using the technologies safely
- School websites
- Using images and digital video on school websites
- Acceptable use of ICT facilities within the school library
- The school as a community resource

Further resources are available on the E-safety section of the Becta Schools website [http://www.becta.org.uk/schools/esafety].

School-wide policies and procedures

Effective policy is the backbone to good practice in schools, and internet safety should be no exception. Good policy, based on actual and prospective scenarios, should help to define strategies for dealing with internet safety incidents should they occur.

While the headteacher should be instrumental in developing such policies and practices, it is suggested that much of this work be delegated to an internet safety co-ordinator, supported by all the key stakeholders.

When formulating your policy, consider:

- ✓ Does the school have a suite of internet safety policies?
- ✓ Who is responsible for the internet safety policies? Has the headteacher nominated a member of staff with responsibility for co-ordinating all internet safety issues?
- ✓ Is the policy supported by all stakeholders – governors, senior management team, librarian, network manager, classroom teachers, pupils and parents?
- ✓ Is the policy linked to other school policies – for example, child protection, health and safety, anti-bullying policies and guidance on copyright and plagiarism?
- ✓ Is the policy supported by clear procedures should incidents of misuse occur? Are all staff aware of their individual responsibilities in responding to certain types of incident?
- ✓ Is the policy regularly reviewed and updated?
- ✓ Is the school's policy consistent with local policies and partnerships?

Communication with parents and carers

Parents and carers should be fully consulted on internet safety issues, and, where possible, should be involved in the development of school policies in this area, for example, through a parental representative on the school's internet safety policy team.

It is essential that schools communicate with parents, informing them of the precautions the school is taking to ensure a safe ICT learning environment, and making them aware of the standards of behaviour and acceptable use of ICT that their children are expected to abide by when at school. Effective communication with parents regarding ICT use in school, through distribution of the acceptable use policy or perhaps via special workshops, reinforces the safety messages taught in school and alleviates some of the fears associated with the use of new technologies.

While there is no statutory requirement for parents to sign acceptable use policies, schools may wish to consider this option. A signed acceptable use form, administered as part of the enrolment process or as part of the home–school agreement, acknowledges the fact that a parent has received the information, and that they and their children are aware of the rules. It may be appropriate for older students to agree to the rules themselves. However, the language of the rules must be appropriate to the age and understanding of the children.

Parents also have a key role to play in the internet safety education of their children, through promoting internet safety at home. ICT offers the opportunity for children and their parents to learn together, and internet safety is an excellent topic that can encourage home–school links. Schools may wish to share information about good practice with parents or carers in order to further embed safety messages and achieve consistency between safety guidelines in the home and the school, possibly running parents' workshops or presentations as part of parents' evenings.





Communication with parents and carers continued…

When formulating your policy, consider:

- ✓ Are parents encouraged to be involved in the creation of internet safety policies, possibly through representation on the school's internet safety policy team?
- ✓ Does the school send information to parents regarding ICT use in school?
- ✓ Are parents aware of the standards that their children are expected to abide by when using the internet and related technologies at school?
- ✓ Does the school provide advice and support on using ICT in the home?
- ✓ Are parents actively encouraged to become involved in school internet safety education programmes?

It is recommended that parental consent for use of images of pupils is gained as a separate exercise – see the checklist for using images and digital video on school websites for further information.

Acceptable use guidelines for staff

Schools may wish to provide guidelines for staff on how they may use the school's ICT facilities. This is as much for staff protection as for disciplinary purposes.

When formulating your policy, consider:

- ✓ Does the school provide a clear policy on acceptable use of internet, email and other ICT facilities by staff? Are staff required to sign the policy as acceptance of its terms?

  The policy should cover appropriate use for work purposes, appropriate use for personal purposes (if at all), and ways in which use will be regulated, and should mention that there will be sanctions for misuse.

  The Information Commissioner provides guidance on developing a policy for the use of electronic communications in The Employment Practices Data Protection Code: Part 3: Monitoring at work [http://www.informationcommissioner.gov.uk]. Use the search facility to locate the document.

  Your LEA may also be able to provide further guidance on this issue.

- ✓ Does the school provide guidance to staff on the appropriate taking of images, their storage on the school's network (or any other media), and rights of access?

  Consider, for the protection of staff, whether it is appropriate for staff members to use personal digital cameras or camera phones on field trips, and how such images should be transferred back to the school. Schools may wish to develop a centralised area on the school's network for storing digital images of pupils, with suitable security for accessing the images, along with a deletion policy for when images are no longer required, or the pupil has left the school.

Acceptable use guidelines for staff continued…

✓ Do all staff have their own email addresses? If so, what measures are in place to minimise the risk of staff receiving unsolicited or malicious emails (particularly if the address is available to pupils, or could be easily guessed outside the school environment)?

✓ Does the school require a standard disclaimer to be attached to all email correspondence, stating that the views expressed are not necessarily those of the school or the LEA?

✓ Is anti-virus protection provided on all staff machines? Is it regularly reviewed and updated? Are staff aware of the measures they must personally take to protect against viruses, for example, checking removable media (floppy disks, CD-ROMs and USB storage devices)? Is there a clear procedure for reporting problems?

The E-safety section of the Becta Schools website provides further information on viruses.

✓ Are staff aware of the procedures for reporting accidental access to inappropriate materials, for example immediately reporting the breach to their line manager or the headteacher?

✓ Are there a range of sanctions in place for deliberate access to inappropriate materials by staff? Are these levelled to the seriousness of the offence (for example immediate suspension, possibly leading to dismissal and involvement of police for very serious offences)?

✓ Does the school take reasonable measures to monitor the use of the internet and email by staff? Is this monitoring transparent, and are staff aware of sanctions for misuse? Also, is the school aware of its responsibilities when monitoring staff communications under current legislation such as:

- Data Protection Act 1998
  http://www.hmso.gov.uk/acts/acts1998/19980029.htm
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
  http://www.hmso.gov.uk/si/si2000/20002699.htm
- Regulation of Investigatory Powers Act 2000
  http://www.hmso.gov.uk/acts/acts2000/20000023.htm
- Human Rights Act 1998
  http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Your LEA may be able to provide further guidance on monitoring ICT use.

✓ Are all staff aware of their individual responsibilities to protect the security and confidentiality of school networks? This may include ensuring that passwords are not shared, and making sure that workstations are not left unattended when a user is logged in.

✓ Do staff have laptops? If so, consider whether any additional guidelines are needed. Also consider the issues relating to personally owned ICT devices used on school premises or at school-related activities, or school-funded devices that are used anywhere: for example, a school laptop used illegally at home, or a personal laptop used for school purposes.





Acceptable use guidelines for pupils

While no technological solution can be 100 per cent effective in guaranteeing safety when using the internet and related technologies, technology can help to minimise the risks to pupils, particularly when supported by a clear acceptable use policy and appropriate internet safety education.

When formulating your policy, consider:

- ✓ Are pupils involved in the creation of school internet safety policies, possibly through pupil representation on the school's internet safety policy team?
- ✓ Does the school have filtering systems in place to prevent pupils from accessing inappropriate materials? Are these systems regularly reviewed and updated?

  The E-safety section of the Becta Schools website provides further information on internet filtering systems and filtering pupils' access on the internet.
- ✓ Are pupils aware of the procedures for reporting accidental access to inappropriate materials?
- ✓ Are there a range of sanctions in place for deliberate access to inappropriate materials? Are these levelled to the seriousness of the offence (for example temporary suspension of ICT rights for minor offences, ranging to permanent exclusion and involvement of the police for very serious offences)? Are pupils aware of these sanctions?
- ✓ Is anti-virus protection provided on all machines? Is it regularly reviewed and updated? Are all pupils aware of the measures they must personally take to protect against viruses, for example, checking removable media (floppy disks, CD-ROMs and USB storage devices)? Is there a clear procedure for reporting problems?

  The E-safety section of the Becta Schools website provides further information on viruses.
- ✓ Does the school have policies on the use of email by pupils? How are email addresses handled (group or individual)? Are webmail accounts permitted? Is use of school email accounts permitted for personal use, or only to support classroom activities?

  The E-safety section of the Becta Schools website provides further information on using email in schools.
- ✓ Does the school take reasonable measures to monitor the use of the internet and email by pupils? Are there individual logins? Is monitoring transparent, and are pupils aware of sanctions for misuse of school facilities?
- ✓ Are pupils aware of their individual responsibilities to protect the security and confidentiality of school networks and external networks? This may include ensuring that passwords are not shared, and incorporating a statement that pupils must not try to deliberately access the online files or folders of their peers, teachers or others (for example, through hacking).
- ✓ Are pupils aware of their social responsibilities with regard to using the internet and related technologies, including treating others with respect?
- ✓ Are all security measures reviewed regularly against the perceived risks to pupils and the latest technology available?

Internet safety skills development for staff

Internet safety awareness should be based on an ongoing programme of education within the school, and staff should not be excluded. In order to assist children and young people to stay safe when using the technologies, it is vital that staff are aware of the issues, both existing and emerging.

When formulating your policy, consider:

- ✓ Do staff receive information and training on internet safety issues and new and emerging technologies on a regular basis? Is this training tailored to their particular role in the school (for example, a network manager will need very different training from a classroom teacher, who in turn will require different training from the child protection liaison officer)?
- ✓ Is there a clear process for supporting staff in their internet safety skills development?
- ✓ Is there a clear process for staff to report any difficulties or concerns which they might encounter?
- ✓ Do staff receive training on information literacy skills (for example, how to search and evaluate information effectively)?
- ✓ Do new staff receive information on the school's acceptable use policy as part of their induction process, and sign to confirm their acceptance of the terms?
- ✓ Are staff encouraged to incorporate internet safety activities and awareness within their curriculum areas? If so, are these activities monitored, supported and co-ordinated across the school?

Internet safety skills development for pupils

The requirement to raise awareness in children and young people of the risks associated with inappropriate contact via the internet and content on the internet is addressed as part of the wider duty of care to which all teachers are bound. It is essential that all pupils are taught the relevant skills and strategies to remain safe when using the internet and related technologies. This may be as discrete internet safety lessons, as part of the ICT curriculum, or embedded within all curriculum work wherever it is relevant.

When formulating your policy, consider:

- ✓ Are pupils given an opportunity to contribute to school internet safety policies?
- ✓ Are pupils and their parents provided with a copy of the acceptable use policy/rules for ICT use when the pupil joins the school? Is it appropriate to the pupil's age and prior exposure to ICT?
- ✓ Are pupils reminded of internet safety rules each time they use the technology?
- ✓ Does the school have a policy/framework for teaching internet safety skills?
- ✓ Does the school provide appropriate opportunities within a range of curriculum areas to teach about internet safety?
- ✓ How does the school go about educating pupils of the dangers of technologies which they might encounter outside school?
- ✓ How is pupils' understanding of internet safety issues assessed or measured?
- ✓ Are pupils aware of relevant legislation when using the internet, such as that relating to data protection and intellectual property, which may limit what they want to do, but also serves to protect them?
- ✓ Are pupils aware of the impact of online bullying, from the perspective of both the victim and the tormentor? Do they know where to seek help if affected by these issues?





Internet safety skills development for pupils continued…

The E-safety section of the Becta Schools website provides further information on online bullying.

✓ Are pupils aware of where to seek help and advice if they experience problems when using the internet and related technologies, for example, their teacher, parents, carers, or organisations such as ChildLine [http://www.childline.org.uk]?

Using the technologies safely

Schools may wish to consider their specific stance with regards to the following technologies. Even if certain technologies are not used within the school environment, it is likely that pupils will use the technologies outside school. Schools may also wish to consider the level of internet safety education they will give to pupils on each of these topics, and where this might take place within the curriculum.

The staff training programme should also cover this information for all school staff.

When formulating your policy, consider:

Internet

✓ What are the restrictions placed on internet use within school?

✓ Are there individual logins and security time-outs?

✓ Does the school use a safe list of websites, or is access filtered?

✓ Are pupils taught how to critically evaluate materials as well as learning good searching skills?

✓ Are pupils taught the importance of intellectual property regarding materials they find on the internet?

✓ What is the school's policy on downloading materials from the internet? Are there different guidelines for different types of materials – for example, copyright-free materials to support classroom work can be downloaded, but downloading of games and music is prohibited?

Email

✓ Do pupils have access to email in school? Is this via group or individual addresses?

✓ If pupils do have an individual email address in school, what are the restrictions on use? For example, can it be used for work-related correspondence only or for personal use? Is email use monitored, and are pupils aware of this?

Using the technologies safely continued…

- ✓ Are pupils aware of the school's policies on email attachments?
- ✓ Do pupils know how to virus-check attachments, both incoming and outgoing?
- ✓ Are pupils aware of the seriousness of bullying by email? Is this incorporated in the school's anti-bullying policy?
- ✓ Are all pupils aware that there are sanctions for misuse of email on the school's network?

The E-safety section of the Becta Schools website provides further information on using email in schools.

Webmail

- ✓ What is the school's policy on webmail services? Are they blocked on the school's network?
- ✓ Do pupils know how to use webmail services safely outside school, for example by looking for privacy statements when registering for webmail accounts?
- ✓ Do pupils know how to use inbuilt junk mail filters within webmail services?

Spam and spoofing

- ✓ Are pupils aware of the issues surrounding spam and spoofing?
- ✓ Are pupils taught appropriate strategies for recognising and dealing with spam?
- ✓ Are technological systems employed within school to help minimise spam?

The E-safety section of the Becta Schools website provides further information on spam and spoofing.

Chat rooms

- ✓ Are pupils aware of the safety issues relating to using chat rooms?
- ✓ Are pupils aware how to safely negotiate online relationships?
- ✓ Are pupils aware of the importance of keeping personal information private when chatting?
- ✓ Are pupils aware of the dangers of arranging offline meetings with people they have met online?
- ✓ Is use of chat rooms permitted within school? If so, is this for classroom use only?

The E-safety section of the Becta Schools website provides further information on using chat in the classroom.

Instant messaging

- ✓ Is access to instant messaging services permitted within school? If not, are such services appropriately blocked on the school's network?
- ✓ Are pupils aware of the safety issues relating to instant messaging?
- ✓ Do pupils know how to protect personal information when registering for instant messaging services, and how to set up closed groups or buddy lists?
- ✓ Do pupils know where to get help and advice if they experience problems such as unwanted messages or bullying by instant messaging?

Mobile phones and other portable devices

- ✓ Are pupils aware of the safety issues relating to mobile phones and other portable communications devices, such as personal digital assistants (PDAs)? Risks include always being accessible (and hence exclusion from other forms of social contact), inappropriate and unsolicited contact by text message, text overuse and misuse, and bullying by mobile phone.
- ✓ Are pupils aware of the new forms of service and content increasingly available via mobile phones, such as picture





Using the technologies safely continued…

and video messaging, Bluetooth, commercial content, and location-aware services, and the safety issues relating to these?

- ✓ Do pupils know how to protect themselves from mobile phone theft? Are they aware of procedures for reporting the IMEI (International Mobile Equipment Identity) number, hence disabling the phone if it is lost or stolen?
- ✓ Are mobile phones permitted within school?
- ✓ If mobile phones are permitted in school, does the school provide guidelines on how and when they can be used? What are the sanctions for misuse?
- ✓ If mobile phones are not permitted within school, how will the policy be enforced?

The E-safety section of the Becta Schools website provides further information on mobile phones.

Camera phones

- ✓ Are pupils aware of the safety issues relating to camera phones, for example having their photograph taken without their knowledge or permission?
- ✓ Are camera phones permitted within school?
- ✓ If camera phones are permitted in school, does the school provide guidelines on how and when they may be used? What are the sanctions for misuse?
- ✓ If camera phones are not permitted within school, how will the policy be enforced?

The E-safety section of the Becta Schools website provides further information on camera phones.

Webcams

- ✓ Are webcams used within school for curriculum activities such as video conferencing? If so, are pupils aware of the appropriate behaviours to adopt when using them?
- ✓ Are pupils aware of the issues of using webcams outside school, such as inappropriate contact and Trojan horses which might activate a webcam without their knowledge?

The E-safety section of the Becta Schools website provides further information on webcams.

Peer-to-peer networks

- ✓ Is access to peer-to-peer services permitted within school? If not, are such services appropriately blocked on the school's network?
- ✓ Are pupils aware of the safety issues relating to peer-to-peer networks?
- ✓ Are pupils fully aware of the risks of viruses, and of the need to virus-check any materials downloaded and install firewalls to protect their own machines?
- ✓ Are pupils aware of their responsibilities with regards to illegally downloading or uploading materials to peer-to-peer networks?

ePortfolios

- ✓ Has the school identified the appropriate levels of privacy on personal data contained within ePortfolios, and has guidance been distributed to staff, pupils and parents – that is, who can see what, when and for how long?
- ✓ Are systems in place to ensure the ethical use of data collected?
- ✓ Are systems in place to ensure the validity of the information contained within ePortfolios?
- ✓ Does the school have/require a 'gatekeeper' for ePortfolios?

© Europortfolio[3]

[3] Thanks to Maureen Layte and colleagues at Europortfolio, the European Consortium for the ePortfolio, for guidance in this area.

School websites

The school should establish clear policies to ensure that its website is effective, and does not compromise the safety of the pupils or staff.

When formulating your policy, consider:

- ✓ Does the school have its own website? If so, is there a senior member of staff responsible for the school's website?

  E-safety section of the Becta Schools website provides further information on safety issues for school websites.

- ✓ Are there clear policies and approval processes regarding the content that can be loaded to the school's website?
- ✓ Are pupils involved with the actual loading and maintenance of content on the school's website? Do they have clear guidelines? Is their work thoroughly checked?
- ✓ Is the website regularly checked to ensure that there is no content that compromises the safety of pupils or staff?
- ✓ Does the school adopt safe practices regarding the publication of images and names of pupils on its website? See the following checklist for further information.
- ✓ Does the school's website make use of a webcam? If so, are safety measures in place to prevent misuse, accidental or otherwise?

  The E-safety section of the Becta Schools website provides further information on webcams.

- ✓ If the school's website uses facilities such as guestbooks, noticeboards or weblogs, are they checked to ensure that they do not contain personal details?

  The E-safety section of the Becta Schools website provides further guidance on weblogs and safety issues for school websites.

- ✓ Does the school allow pupils to create their own websites on the school's network? If so, can the school ensure that they adhere to all of the above points?
- ✓ Can the school be certain that it is not infringing the intellectual property rights of others through any of the materials available via its website? Copyright may apply to text, images, music or video that originate from other sources. How will the school protect its own copyright in terms of the materials it publishes on its website?





Using images and digital video on school websites

Including images of pupils on the school's website can be motivating for the pupils involved and provide a good opportunity to promote the work of the school. Schools therefore need to develop a policy in relation to the use of images of pupils on the school's website. The head and governors will need to make decisions about the type of images they consider suitable and that appropriately represent the school. They will want to ensure that parents support their policy. Further guidance may also be available from the LEA.

Schools should also give consideration to the way in which digital images and video are captured and stored within the school, and develop guidelines for the protection of both pupils and staff. Consider, for the protection of staff, whether it is appropriate for staff members to use personal digital cameras or camera phones on field trips, and how such images should be transferred back to the school. You may wish to develop a centralised area on the school's network for storing digital images of pupils, with suitable security for accessing the images, along with a deletion policy for when images are no longer required, or the pupil has left the school.

When assessing the potential risks in the use of images of pupils, the most important factor is the potential of inappropriate use of images of children.

Considerations include:

- ✓ Does the school ask for parental permission before using images of pupils, whether on the school's website or elsewhere? This ensures that parents are aware of the way an image of their child is representing the school. A parental consent form is one way of achieving this.
- ✓ Avoid using the first name and last name of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside school. An easy rule to remember is:
  - If the pupil is named, avoid using their photograph.
  - If a photograph is used, avoid naming the pupil.
- ✓ Consider using group photos rather than photos of individual children.
- ✓ Ensure that the image file is appropriately named – do not use pupils' names in image file names or ALT tags if published on the web.
- ✓ Ensure that images are appropriately stored and secured on the school's network.
- ✓ Only use images of pupils in suitable dress to reduce the risk of inappropriate use.
- ✓ Create a recognised procedure for checking the website, reporting the use of inappropriate images to reduce the risks to pupils, and responding to any such report.

The E-safety section of the Becta Schools website provides further information on using images and digital video on school websites, and includes sample permission forms.

Acceptable use of ICT facilities within the school library

Several factors can make the creation of a safe ICT learning environment more complex and challenging in a school library than in the classroom or ICT suite.

When formulating your policy, consider:

- ✓ Is a separate or additional acceptable use policy required for library use? If so, are pupils involved in the process of creating it?
- ✓ Are there any different technologies or services that pupils might encounter in the library that need additional guidance?
- ✓ Are the library computers provided for education use only, or is some personal use by pupils permitted?
- ✓ Are teachers aware of their responsibilities with regard to supervising pupils' use of library ICT facilities during class time? How is this information communicated to staff members?
- ✓ How will individual pupil's use of ICT facilities in the library be controlled, particularly when the librarian may not know the identity of all pupils? Do pupils need to pre-book machines and sign in to use them? Will pupils' use of ICT facilities be limited during busy times? How is this information communicated to pupils?
- ✓ Are all library staff clear of the procedures they must follow if misuse of ICT facilities occurs in the library, including reporting to the internet safety co-ordinator and liaising with the network manager to advise on filtering and blocking as necessary?
- ✓ Are procedures in place for supporting pupils who wish to engage in legitimate research via the internet, but who face barriers due to filtering and blocking provisions on the school's/library's network?
- ✓ What role does the school library play in developing pupils' information handling and information literacy skills?
- ✓ Is the design of the library such that internet-accessible computers can be positioned in view of the librarian's workstation? Can the layout be improved within the space and technology constraints of the library environment?

The school as a community resource

Schools are increasingly used as a community resource, and such use should also be covered by internet safety policies.

When formulating your policy, consider:

- ✓ Are the school's ICT facilities ever used as a community resource?
- ✓ What use is made of the facilities, and who takes responsibility for this?
- ✓ Is information on ICT use and internet safety contained within the school's lettings policy?
- ✓ How can you ensure that community users of school ICT resources sign a (tailored) acceptable use policy? How will the process be managed?
- ✓ How will existing technological solutions to internet safety impact upon community use? Will filtering and blocking profiles used during the school day be too restrictive? Can these restrictions be varied by factors such as time of access or password?
- ✓ How will community use of school ICT facilities be monitored?
- ✓ How will incidents of misuse by reported and managed?





Appendix 4: Notes on securing and preserving evidence

School premises

Following any incident that may indicate that evidence of indecent images or offences concerning child protection may be contained on school computers, the matter should be referred at the earliest opportunity to the local police station.

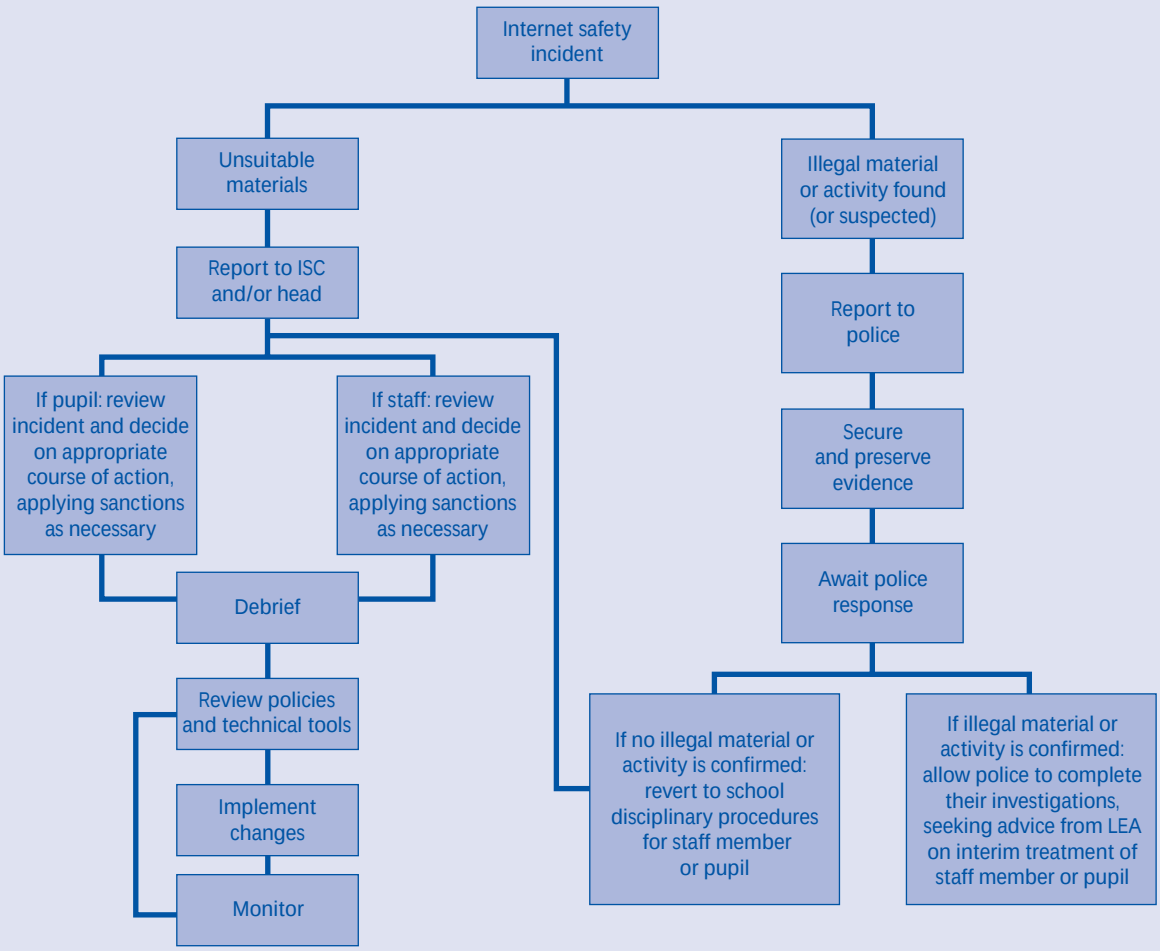
There are many instances where schools, with the best of intentions, have commenced their own investigation prior to involving the police. This has resulted in the loss of valuable evidence both on and off the premises where suspects have inadvertently become aware of raised suspicions. In some circumstances this interference may constitute a criminal offence also.

The police will be interested in obtaining 'best evidence'. This, in reality, will be to forensically copy computers that may contain evidence of offences. This act can be carried out discreetly out of hours to have a minimal impact on the school. If the school identifies a suspect computer, it should not be used or viewed and advice can be sought from the local police hi-tech crime unit via their local police station.

Home computers

If a student discloses potential crimes involving computer-based media, again the police will normally look to obtain a forensic copy of the student's home computer to preserve any evidence. This will be conducted discreetly and, in many cases, the computer will be returned quickly. However, the point must be made that the impact on the family could have far reaching consequences should illegal material be discovered.

Flowchart for responding to internet safety incidents in school





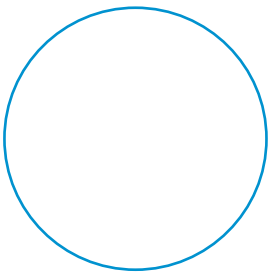


Appendix 5: Glossary

Acceptable use policy (AUP)	A policy that a user must agree to abide by in order to gain access to a network or the internet. In the schools context, it may also cover how other communications devices, such as mobile phones and camera phones, can be used on the school premises.
ALT tag	ALT tags, or alternate text tags, are typically used to provide further detail on an image on a web page. The text is seen when the image is being loaded, and is also often seen when a mouse is passed over the image.
Blog	A blog, also known as a weblog, is a form of online diary or journal. Blogs contain short, frequently updated posts, arranged chronologically with the most recently posted item appearing at the top of the page. In addition to text, blogs can contain photos, images, sound, archives and related links, and can incorporate comments from visitors.
Bluetooth	Bluetooth is a telecommunications industry standard which allows mobile phones, computers and PDAs to connect using a short-range wireless connection.
Bookmarking	The process of storing the address of a website or internet document on your computer, so that you can find it again easily.
Caching	The process of temporarily storing files, such as web pages, locally to enable quick access to them in the future without placing demands on network resources.
Chatroom	An area on the internet or other computer network where users can communicate in real time, often about a specific topic.

Digital video	Video captured, manipulated and stored in a digital format.
Filtering	A method used to prevent or block users' access to unsuitable material on the internet.
Firewall	A network security system used to restrict external and internal traffic.
Hacking	The process of illegally breaking into someone else's computer system, breaching the computer's security.
Information and communications technologies (ICT)	The computing and communications facilities and features that, in an educational context, variously support teachers, learning and a range of activities.
Information literacy	The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.
International Mobile Equipment Identity (IMEI)	A unique 15-digit serial number for mobile phones. When a phone is lost or stolen the number can be identified as invalid, so rendering the handset useless. It can be found by keying *#06# on your phone's keypad.
Internet service provider (ISP)	A company providing a connection to the internet and other services, such as browser software, email, a helpline, web space and subscriber-only content.
Personal digital assistant (PDA)	A small, mobile, handheld device that provides computing and information storage/retrieval capabilities, and possibly phone facilities too.
Spam	Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.
Spoofing	Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.
Trojan horses	A virus which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.
Video conferencing	The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.
Virus	A computer program which enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.
Webcam	A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.
Weblog	See the entry for 'blog', above.




01/DD05-06/2029/175/MP/12k

Becta
ICT Advice

British Educational Communications and Technology Agency (Becta)

Millburn Hill Road, Science Park,
Coventry CV4 7JJ
Tel: 024 7641 6994
Fax: 024 7641 1418

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