

DRAFT



Schools e-Safety Policy 2007

**A template to help schools
write their own policy**

January 2007

Kent Local Authority believes that the benefits of ICT and Internet use in schools far outweigh the dangers. Recognising the issues and planning accordingly will help to ensure appropriate, effective and safe pupil use. Where schools wish to write an e-Safety Policy, this template will promote discussion and accelerate writing.

KCC Children, Families and Education Directorate has also approved core policies for both Primary and Secondary Schools where a ready to use policy is required.

**KCC Children, Families and Education Directorate with Kent Schools,
Child Protection, EIS, SEGfL and Kent Police.**



CONTENTS

1. Introduction

- 1.1 What is e-safety?
- 1.2 What can an e-safety policy provide?
- 1.3 How do I use the policy template?
- 1.4 Statement of authority
- 1.5 School staff
- 1.6 Routes to e-safety – Primary
- 1.7 E-safety for pupils with additional needs
- 1.8 Routes to e-safety – Secondary
- 1.9 Response to an incident of concern

2. School e-safety policy questions

- 2.1 Who will write and review the policy?
- 2.2 Teaching and Learning
 - 2.2.1 Why is Internet use important?
 - 2.2.2 How does Internet use benefit education?
 - 2.2.3 How can Internet use enhance learning?
 - 2.2.4 How will pupils learn how to evaluate content?
- 2.3 Managing Information Services
 - 2.3.1 How will information systems security be maintained?
 - 2.3.2 How will e-mail be managed?
 - 2.3.3 How will published content be managed?
 - 2.3.4 Can pupil images and work be published?
 - 2.3.5 How will social networking and personal publishing be managed?
 - 2.3.6 How will filtering be managed?
 - 2.3.7 How will videoconferencing be managed?
 - 2.3.8 How can emerging technologies be managed?
 - 2.3.9 How should personal data be protected?
- 2.4 Policy Decisions
 - 2.4.1 How will Internet access be authorised?
 - 2.4.2 How will reported incidents be managed?
 - 2.4.3 How will risks be assessed?
 - 2.4.4 How will complaints be handled?
 - 2.4.5 How should the Internet used across the community?
- 2.5 Communications Policy
 - 2.5.1 How will the policy be introduced to pupils?
 - 2.5.2 How will the policy be discussed with staff?
 - 2.5.3 How will parents' support be enlisted?

3.0 Supporting Materials (published on www.clusterweb.org.uk?esafety)

- Core e-safety policies for primary and secondary schools
- Responsible Use Posters for Key Stage 1, Key Stage 2 and Secondary
- Acceptable ICT Use Agreement for staff
- Sample letter to parents and consent forms

4.0 e-Safety contacts and references

5.0 Acknowledgments

6.0 Legal framework

Schools e-Safety Policy 2007

Sixth Edition
January 2007

1.1 Why write an e-safety policy?

Pupils interact with the Internet and other communications technologies such as mobile phones on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas and social interaction are both greatly beneficial but can occasionally place young people in danger.

Schools must decide on the right balance between controlling access, setting rules and educating students for responsible use. Parents, libraries and youth clubs must develop complementary strategies to ensure safe and responsible ICT use wherever young people may be.

Teachers and officers have produced this template to help schools to write their own e-safety policies. To encourage debate, the template offers a range of responses to common policy questions as well as a discussion of effective practice in schools.

Ready made core e-safety policies approved by the Children, Families and Education Directorate are also available for immediate use.

E-safety comprises all aspects relating to children and young people and their safe use of the Internet, mobile phones and other technologies, both in and out of school. It includes education on risks and responsibilities and is part of the 'Duty of Care' which applies to everyone working with children. A new national e-safety drive is being led by the Child Exploitation and Online Protection Centre (CEOP).

Many individual schools and local authorities across the UK have used earlier editions of the Kent materials. This new edition incorporates experience gained in schools and advice from child protection officers, Kent Police and the South East Grid for Learning. Further suggestions are always welcome.

This policy template, posters and forms may be copied and adapted for non-profit, educational purposes, providing KCC copyright is acknowledged. It would be helpful if readers outside Kent could inform us by e-mail when they use these materials.

Peter Banbury, Editor
peter.banbury@kent.gov.uk

Rebecca Chapman, e-Safety Officer.
rebecca.chapman@kent.gov.uk

© Kent Children, Families and Education Directorate, January 2007.

Latest copy: www.clusterweb.org.uk?esafety

Kent County Council and its employees do not accept responsibility for any loss of any kind caused to any person as a result of reliance on the content of this publication. You are advised to take independent advice on the merits of any individual course of action that you wish to undertake.

1.2 What is e-safety?

The Kent Schools Internet Policy has been renamed as the Kent Schools e-Safety policy to reflect the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

The Internet is an open communications channel, available to all. Applications such as the Web, e-mail, blogs and social networking all transmit information over the fibres of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security.

Schools need to protect pupils and staff but also to protect themselves from legal challenge. The law is catching up with Internet developments: it is an offence to store images showing child abuse and to use Internet communication to 'groom' children. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken to protect users.

1.3 How do I use the policy template?

Teachers will be aware of the risks of Internet use but may not have had opportunities for detailed discussion. This policy template can assist the writing process without bypassing the essential debate. For a staff meeting, the policy template may be viewed from the Web or downloaded for editing.

When writing your policy, educational, management and technical issues will need to be considered. These are presented as questions with discussion and a range of suggested statements. The writing team should consider each question and select statements appropriate to the school context, or use these as templates for editing.

Some schools may feel they do not have the expertise to write their own policy. CFE has also provided core policies for primary and secondary schools on the e-safety site which can be quickly edited for approval by SMT and Governors.

Government guidance in areas such as e-mail, social networking and publishing continues to evolve. Schools should also consult the Becta guidance:

<http://www.becta.org.uk/schools/esafety>

Schools should review their policy regularly and revise the policy annually to reflect changes and advancements in technology. School ICT use is changing rapidly and policies produced a year ago will already be out of date.

1.4 Statement of authority

This document has been written by teachers and officers to reflect effective practice, to raise issues and to point to sources of expert knowledge. The contents have been discussed with Kent Police and the Children's Safeguards Service with additional comment from national groups such as Becta and the Child Exploitation and Online Protection centre (CEOP).

Through this Policy, the KCC Children, Families and Education Directorate is making a strong statement as to the precautions that it expects schools to take. Schools complying with this Policy will more easily be able to demonstrate that they have taken reasonable steps to protect their pupils, should a serious problem arise.

Statements strongly recommended by Kent are shown by the red **K**

Kent schools have the primary responsibility for e-safety and must consider the issues raised in this document. An e-safety audit is recommended, possibly using external expertise, to ensure all reasonable steps have been taken.

This is not, of course, your school's e-safety policy. This should be written by the headteacher and staff after reviewing this document, consulting the reference material and discussing with the staff what is appropriate in your school.

1.5 School staff

IT applications are developing rapidly and can leave staff unsure of their use or how to react when pupils discuss their Internet use. Advice and training may be obtained from the e-safety officer, advisers or child protection officers.

The trust between pupils and school staff is essential to education but occasionally breaks down. This is not new, but has been highlighted by better awareness of human failings and greater respect for children. The new Child Exploitation and Online Protection centre (CEOP) has been set up by the Home Office to "safeguard children's online experiences and relentlessly track down and prosecute offenders".

In industry and indeed KCC, a member of staff who flouts IT security advice, or uses email or the Web for inappropriate reasons risks dismissal. Sadly a few school staff have disregarded their responsibilities and some have been dismissed.

All staff should sign an Acceptable ICT Use Agreement on appointment. In signing, staff accept that the school can monitor network and Internet use to help ensure staff and pupil safety.

Staff who manage filtering and monitor ICT use have great responsibility and must be managed appropriately. Procedures must define how inappropriate or illegal ICT use is reported to senior management. Staff must be aware of dangers to themselves in managing ICT use, for instance in viewing inappropriate images to investigate their source. Section 6.4 of this document is helpful.

Any allegation of inappropriate behaviour must be reported to senior management and investigated with great care - an innocent explanation may possibly exist.

Email, text messaging and IM (Instant Messenger) all provide additional channels of communication between staff and pupils and inappropriate behaviour can occur. Staff should realise the power of the technology in Police hands to identify the sender of inappropriate messages. Some schools are using school-owned, phones for staff-pupil contact to ensure monitoring to protect staff from false accusations.

1.6 Routes to e-safety - primary

A very present danger

Despite precautions at school, open access to the Internet has become an integral part of children's lives. A growing danger is presented by the ease of uploading material to the Web. We already have evidence from Kent schools of primary pupils' use – at home – of social networking sites such as Bebo and Piczo, which allow children to set up an account and create a web page in minutes. Information given by users is not checked and there appears to be a total lack of safeguards. Children are being told (often by teenagers) to look at their sites.

We suggest that primary pupils are alerted to the dangers in this way:

If one of your friends, or an older person, tells you about a site they want you to see, think carefully. If someone sends you a link, don't open it unless you are sure it's safe. If you are worried, tell a teacher or an adult in your family.

Advice in section 2.3.4 applies in all settings. Pupils should not upload photographs or videos of themselves or other pupils. They must not publish personal information, such as location and contact details. Consideration should be given to advising pupils to use an anonymous "cyber name" where logging into sites is essential.

Identifying vulnerable groups

Many primary pupils have access to mobile devices. The use of handhelds and internet-enabled mobile phones both inside and outside school is increasing rapidly. The most ICT capable may be the most vulnerable. They may not be the most academically gifted. Children who interact poorly socially may be more at risk from inappropriate online contact.

- Schools should ensure that a copy of the School's e-Safety Policy is sent to parents and governors.

Using the Internet to support learning

Most Internet use in primary schools is safe, purposeful and beneficial to learners. There is always an element of risk: even an innocent search can occasionally turn up links to adult content or violent imagery. Risks are magnified by the upsurge in schools' Internet access. However, many teachers feel that there is a far greater problem in the amount of irrelevant, incomprehensible material typically yielded by Web-wide searches.

For the youngest pupils, the greatest risk is through inadvertent access. Fast broadband means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content. A procedure should be agreed with all staff on what to do, and how to handle the situation with pupils. For example:

Close or minimise immediately. Don't try to navigate away. If pupils saw the page, talk to them about what has happened, and reassure them. Later, investigate the history of visited sites to get details to report, and to find how the pupil got there.

In view of the risks, we advise that primary pupils are supervised at all times when using the Internet. All staff should be aware that networked computers are online at all times when a user is logged on.

Search engines

We urge teachers to think very carefully about allowing primary pupils to use Internet-wide search engines such as Google. If Google is to be used at all, you must make sure that strict filtering is applied. Go to www.google.co.uk and click *Preferences*.

The BBC search engine is a safer approach for children: <http://search.bbc.co.uk/>

Image searches are especially risky. There may be no need for pupils to use them, provided an adult downloads images before the lessons and stores them in a shared folder. Alternatively, teachers may use Microsoft's clipart library, which automatically adds downloaded images to Clipart: <http://office.microsoft.com/clipart/>

Tagged image browsers are fun to explore. A good example is www.airtightinteractive.com/projects/related_tag_browser/. The danger is that this will accept inappropriate keywords. While useful to teachers, we can no longer recommend it for use by pupils. Links such as this must not be stored in 'Favorites' accessible to pupils.

For most curriculum-related research, there is no need to use an unfenced search engine. **Yahooligans**, although US centric, does offer a range of selected sites which are relevant to the UK curriculum. For details, see Yahooligans UK: <http://uk.docs.yahoo.com/yahooligans/parents.html>

There is excellent advice on safe searching at The Guardian's NetClass: <http://education.guardian.co.uk/netclass> (click on 'I can't find what I want'). However, please note that NO filtering-based search engine is completely safe.

The homepage in many Kent schools is RM's www.learningalive.co.uk. This features a Google search box. Great care should be taken as this offers the opportunity to any pupil to go onto a computer in an unsupervised area and search the Internet. Even with strict filtering, unsuitable content was readily found when recently tested on a modern network. A far better starting point is **Pathways**, also accessible from the Learning Alive homepage. Pupils search a 'walled garden' of 4000 approved sites. Each match shows an indication of age range.

Curriculum planning

Good planning and preparation is critical in ensuring a safe starting point for the development of Web search skills and strategies. Tasks can be planned that do not require an Internet-wide search engine.

If the aim is to teach search skills, **BBC Schools** offers a safe environment. The search box automatically restricts the search to the BBC Schools site. There is no indication of age range, but pupils can judge readability from the example retrieved by the search www.bbc.co.uk/schools. Importantly, primary pupils can learn skills such as keyword selection to narrow down searches, and evaluating quality and relevance. This will prepare them for efficient, productive Internet research in the secondary phase.

Webquests contain direct links to support research. There is no need to use a search engine. Some webquests simply consist of a list of questions. The questions are linked directly to text sources and offer a motivating means of engaging reluctant readers in 'finding out'. The homework pages at Woodlands Junior School contain many examples: <http://woodlands-junior.kent.sch.uk/Homework/>

Others are designed to support collaborative group activity. They encourage pupils to apply what they have found, leading to more effective learning. The webquests at WebQuestUK are linked to National Curriculum topics and QCA schemes of work.

DRAFT for COMMENT

They offer a self-contained set of learning tasks with a defined outcome, such as recording a WWII evacuee's diary or writing a Victorian school's handbook.

<http://www.webquestuk.org.uk/>

A list of webquests is at: <http://ecs.lewisham.gov.uk/youthspace/quests/>

The Dragonfly Challenges at Naturegrid draw on the natural habitat 'Explorer' themes and are a useful introduction for Key Stage 2:

www.naturegrid.org.uk/email/enquiry.html

Any teacher able to produce a document in Word can create his/her own webquest! To place an active web link on the page, simply select and copy from the address bar in Internet Explorer, and paste into Word. To follow the link, press and hold the Ctrl key while you click on the link.

Primary school learners need not be exposed to the risks of the unfenced Internet!

Email

Many Kent primary schools use RM EasyMail Plus. This has the facility to restrict pupils' email to sending / receiving within the domain only. Strict filtering is applied and abuse notified. See: www.rm.com/primary/products/product.asp?cref=pd1705

For external email, there is no need for pupils to use individual accounts. A 'class' email address may be set up, and moderated by the teacher. Many schools ensure safety by arranging email exchanges as a class project. For examples and further advice see:

www.kented.org.uk/ngfl/ict/easymail/

www.kented.org.uk/ngfl/ict/email/st-marys/

NB: ICT co-ordinators: keep your administrator account and password details in a safe place. Ensure that someone else will have overall access to school email accounts if you leave!

SuperClubs Plus

Let's consider where we started – the Internet is an integral part of children's lives, whether we like it or not. Fortunately, there is way for learners to experience the benefits of communicating online with their peers, in guaranteed safety.

Subscribers to SuperClubs Plus – successor to the DfES GridClub – are able to access safe, moderated email in a closed group of over 100,000 pupils registered by their schools. Key Stage 2 pupils are also able to set up home pages and join clubs, to share learning and interests. Pupils are encouraged to develop skills in website design and management, and to learn the protocols involved with safe chat.

The site is colourful in design and attractive to young people. Membership is validated by the school, communications are rigorously filtered and live communication is supervised by professional moderators.

Safe online communication develops pupils' ICT and Literacy skills, also their awareness of responsible citizenship and well-being. There is an award scheme, with a 'green star' for children who pass online communication tasks. The service has won the Internet Watch Foundation Award for its 'contribution to a safer Internet'. For details please see:

<http://www.kented.org.uk/ngfl/ict/internetprof/index.htm>

The Cyber Café on the home page is free and will help teach e-safety in an interactive and interesting way, as part of planned e-safety education.

1.7 e-safety for pupils with additional needs

There is an underlying assumption that children have both understanding and application of “safety”. Pupils need to understand that rules given to them must be followed. Pupils need to learn safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. Pupils need to understand that certain rules will change and develop as they get older

Pupils need to learn how to apply strategies that will help them to avoid certain “risks” such that they need to plan ahead.

There are certain aspects of the above that are particularly challenging for pupils with additional needs and children who we may consider to be vulnerable in this learning context. Pupils will clearly have individual needs that will present different issues when teaching e-safety but some common difficulties may be

- They may be still developing their social understanding of safety and so may relate better to strategies used with younger children
- They are likely to find it hard to apply the same rules in different situations
- Most safety principles rely on children being able to explain what happened or to ask for help
- Some children may have poor recall and difficulties with learning through experience.

It would seem to be relevant for all schools to consider their e-safety policy in relation to specific adaptations that may be required for this group of pupils. It may also be helpful for SENCOs to coordinate advice between ICT specialist and support staff.

This may take the form of very child focused strategies that would apply to a pupil with specific needs that would need to be available to all staff implicated in Internet use with that child.

Alternatively, whole school approaches could take into consideration strategies that would support the needs i.e. specific choices of visual support to remind pupils of the rules.

For some advice on strategies regarding teaching e-safety to pupils with additional needs, please refer to the “e-Safety Considerations for AEN” handout on the Clusterweb e-safety page:

<http://www.clusterweb.org.uk?e-safety>

1.8 Routes to e-safety – secondary

The safe and effective use of the Internet is an essential life-skill, required by all pupils and staff. Unmediated Internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. Schools need to write and particularly to implement a policy to ensure responsible ICT use and the safety of pupils in consultation with Staff, Parents, Governors and Students. The e-Safety Policy will work in conjunction with other policies including Student Behaviour, Anti-Bullying and Curriculum.

In writing e-safety policies, secondary schools should consider these core principles:

Guided educational use

Curriculum Internet use produces significant educational benefits including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment in order to enrich and extend learning activities. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth. Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.

Risk assessment

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At an appropriate age they will need to learn to recognise and avoid these risks – to become "Internet Wise".

Schools need to perform risk assessments to ensure that they are fully aware of and can mitigate risks of Internet use. Pupils need to know how to cope if they come across inappropriate material.

Pupils' Internet access may be in Youth Clubs, Libraries, public access points and in homes. Ideally a similar approach to risk assessment and e-safety would be taken in each of these locations. Schools may decide to take a lead in this area.

Responsibility

E-Safety depends on staff, schools, governors, advisers, parents and - where appropriate - the pupils themselves taking responsibility. Staff have a particular responsibility to supervise use, plan access and set good examples. The balance between educating pupils to take a responsible approach and the use of regulation must be judged carefully.

Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied, for instance un-moderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions. Students in some schools devise their own rules for Responsible Internet Use.

DRAFT for COMMENT

The school should keep an up-to-date record of access levels granted to all network users. Parents should be informed that students will be provided with supervised Internet access and parents and students should sign an acceptable use agreement. Senior staff should take responsibility for regularly checking that filtering and monitoring is appropriate, effective and reasonable, and that technical staff have not taken on themselves the responsibility for educational or disciplinary issues.

Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant. The school should take all reasonable precautions to ensure that users access only appropriate material. Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be matched to the age and curriculum requirements of the Student.

However, due to the international scale and linked nature of Internet content, it is impossible to guarantee that unsuitable material will never appear on a school computer.

Principles behind Internet use

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet access is an entitlement for students who show a responsible and mature approach to its use. The school has a duty to provide students with safe and secure Internet access as part of their learning experience. The school Internet access should be designed expressly for student use and will include filtering appropriate to the age of student.

Students need to be taught what is acceptable and what is not and given clear objectives for Internet use.

Internet safety and literacy education

Students will need to be educated in the responsible and safe use of the Internet and other technologies through a range of strategies including:

- The Think U Know training which is extremely powerful and provided without charge via Cluster based INSET sessions from the CFE e-Safety Officer.
- The Becta leaflet "Signposts to Safety" discusses in detail how e-safety themes and ideas can be integrated with subjects across the curriculum.
- Reactive discussion when a suitable opportunity occurs.

Schools should ensure that the use of Internet derived materials by staff and by students complies with copyright law, students should be made aware of plagiarism and issues relating to work research being undertaken for coursework. Staff and students should be trained to become critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

DRAFT for COMMENT

Staff and student electronic communications

Staff and students need to understand that the use of the school's network is a privilege which can be removed should reason arise. The school may monitor all network and Internet use in order to ensure student safety.

All users should be expected to adhere to the generally accepted rules of network etiquette (netiquette). These include but are not limited to the following:

- Be polite.
- Use appropriate language.
- Do not get abusive in your messages to others.
- Do not reveal the personal address, phone number or other personal details of yourself or other users.
- Do not use the network in such a way that would disrupt the use of the network by other users.
- Illegal activities are strictly forbidden.
- Note that e-mail is not guaranteed to be private.
- System administrators have access to all mail.
- Messages relating to or in support of illegal activities may be reported to the authorities.

Using new technologies in education

New technologies should be examined for educational benefit and a risk assessment carried out before use in school is allowed. Secondary schools (and certainly their pupils) are in the forefront of the use of a huge range of new technologies and learning opportunities including:

- Mobile phones with the power of a PC, with Internet, Bluetooth and IR connectivity and a camera.
- New learning environments such as Moodle and the Becta approved learning platforms
- Thinking skills as challenged by games environments and simulations
- Internet voice and messaging such as Skype and IWB linking.
- Digital story telling involving independence of thought and self-motivation
- Podcasting, broadcasting and recording lessons, pervasive digital video

Some of these technologies may disappear, but some will change our world. What is importance is to combine the experimental ability of youth with the wisdom of teachers to develop appropriate, effective and safe uses in teaching and learning.

Web Links

Becta has produced three booklets that are essential reading:

- **Safeguarding children in a digital world** Ref: BEC1-15401
- **E-safety (revised)** Ref: BEC1-15402
- **Signposts to safety** Ref: BEC1-15274 (Particularly KS3 and KS4)
A version for primary schools is being developed.

1.9 Response to an incident of concern

Internet technologies and electronic communications provide children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. However, it is also important to consider the risks associated with how these technologies are used.

An e-Safety Policy should also recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for other users.

These risks to e-safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents.

This section will help staff determine what action they can take and when to report an incident of concern to the school Designated Child Protection Co-ordinator or the e-Safety Officer. Matters can then be handed over to the Children's Safeguards Service or the Police if that becomes necessary.

What does electronic communication include?

- **Internet collaboration tools:** social networking sites and blogs
- **Internet research:** web sites, search engines and Web browsers
- **Mobile phones and personal digital assistants (PDAs)**
- **Internet communications:** e-Mail and instant messaging (IM)
- **Webcams and videoconferencing**
- **Wireless games consoles**

What are the risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Hacking and security breaches
- Corruption or misuse of data

How do we respond?

Child Protection Officers working with the CFE e-Safety Officer have provided guidance should you be concerned about the Internet usage of a child, young person or member of staff.

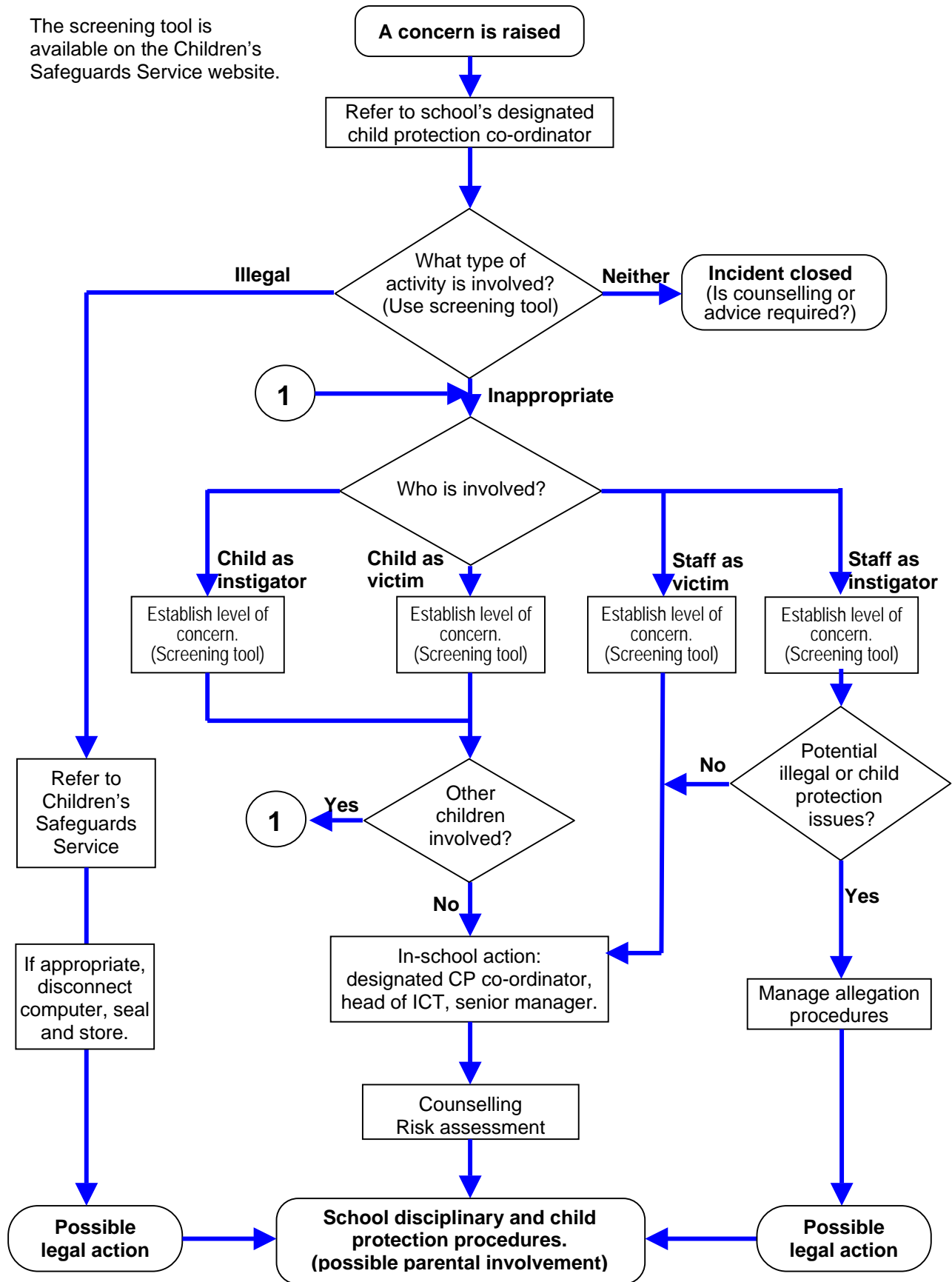
The flowchart on the next page is taken from their material and illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and the Children's Safeguards Service has provided supporting documents to assist schools when responding to incidents.

Please see the Children's Safeguards Service website:

http://www.clusterweb.org.uk/Children/safeguards_home.cfm

Response to an Incident of Concern

The screening tool is available on the Children's Safeguards Service website.



School Responsibilities

As e-Safety is a relatively new concept and a wider responsibility than Internet use, a summary of the schools e-safety responsibilities might be useful. This list should assist the school in developing a co-ordinated and effective approach to managing e--Safety issues.

The following should be considered:

- As Becta recommends, Kent is encouraging each school to appoint an e-Safety Coordinator who will be responsible for dealing with any e-Safety issues that arise. Often this may be the Designated Child Protection Coordinator as the roles overlap, but could also be a member of SMT, the ICT Coordinator or a subject teacher e.g. PSHE or Citizenship. The e-Safety Coordinator will receive support and advice from Kent's e-Safety Officer, the Children's Safeguard Service and where necessary, the Police.
- The e-Safety coordinator should be involved in maintaining the e-Safety policy, will manage e-Safety training and should keep abreast of local & national e-Safety awareness campaigns.
- Schools should review their policy regularly and revise their policy annually to ensure that it is current and includes any emerging technologies used in school.
- Schools should audit their filtering systems regularly to ensure that inappropriate websites are blocked and that pupils and staff are adhering to the policy, by investigating any incidents of misuse.
- Schools should include e-Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Every pupil needs to know how to control and minimise online risks and how to report a problem.
- All staff must read and sign the Acceptable ICT Use Agreement. Whenever the policy changes significantly, a new agreement will be required.
- Parents should sign and return the consent form for Responsible Internet Use.
- All staff, governors, parents and visitors should be given a copy of the policy to read and review.

Implementation and Compliance

No policy can protect pupils by itself. Staff vigilance in planning and supervising appropriate and educational ICT experiences remains essential. The following ideas and checks may be useful:

- Posters by computers will remind pupils of their responsibilities.
- Do staff, pupils and parents know how to report an incident of concern regarding Internet use?
- Where filtering is managed locally, which member of SMT approves the school filtering policy and supervises staff who manage the filtering system?

For further information and an e-Safety audit please visit the e-safety site:

<http://www.clusterweb.org.uk?e-safety>

2 School e-safety policy questions:

Document format: A discussion is followed by one or more possible statements that you might wish to incorporate into your School e-Safety Policy. As statements cover a wide variety of schools, some will be inappropriate in your context. Naturally schools may edit the statements or substitute their own. Please submit any new or improved statements to the editor for inclusion in future editions.

2.1 Who will write and review the policy?

Discussion: The e-Safety Policy is part of the ICT Policy and School Development Plan and should relate to other policies including those for behaviour, personal, social and health education (PSHE) and for citizenship. Policy construction provides a method to review practice, in this case the use of a major technology and its benefits and risks. The more that staff, parents, governors and pupils are involved in deciding the policy, the more effective it will be.

Possible statements:

- K** The school will appoint an e-Safety coordinator. In many cases this will be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors and the PTA.
- The e-Safety Policy will be reviewed annually.

2.2 Teaching and learning

2.2.1 Why is Internet use important?

Discussion: Education develops and responds to society and the Internet and individual communications are having many effects, some profound, on society. Less than ten years ago, we were asking whether the Internet should be used in all schools. Now every pupil is younger than the Internet and the World Wide Web and many use it more than their teachers. Nevertheless it is important to state what we are trying to achieve in education through ICT and Internet use.

Possible statements:

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.2.2 How does Internet use benefit education?

Discussion: The Government has set targets for broadband Internet use in all schools by 2006 and for the use of personal learning spaces by 2008. A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet in education.

Possible statement:

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the LA and DfES;
- access to learning wherever and whenever convenient.

2.2.3 How can Internet use enhance learning?

Discussion: Increased computer numbers or improved Internet access may be provided but effective use and quality of learning must also be addressed. Developing effective practice in Internet use for teaching and learning is essential. Librarians and teachers will help pupils learn to distil the meaning from the mass of information provided by the Web. Often the quantity of information is overwhelming and staff may guide pupils to appropriate Web sites, or develop location skills. Offering younger pupils a few good sites is better than the easy option of a Web search. Above all pupils will learn to evaluate everything they read or see and to take care in their own publishing and interactions with others via the Internet.

Possible statements:

- K** The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- K** Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.2.4 How will pupils learn how to evaluate Internet content?

Discussion: The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop skills in selection and evaluation. The spreading of malicious rumour has occurred for thousands of years and lies can win over truth. Information received via the Web, e-mail or text message requires superlative information handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read. A whole curriculum approach may be required.

In a perfect world, inappropriate material would not be visible to pupils using the Web but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

More often, pupils will be judging reasonable material but will need to select relevant sections. Pupils should be taught research techniques including the use of subject catalogues and search engines and be encouraged to question the validity, currency and origins of information. Key information handling skills include establishing the author's name, date of revision and whether others link to the site. Pupils should compare web material with other sources. Effective guided use will also reduce the opportunity pupils have for exploring unsavoury areas.

Alan November's site is useful: <http://www.anovember.com/>

Access to sensitive sites, for example those that record the Holocaust, may be required for the duration of a specific educational activity by supervised pupils of appropriate age. Some filtering software can provide temporary access to specific sites, which a teacher considers necessary for a particular purpose.

Clearly pupils need to understand that unselective copying is worth little without a commentary that demonstrates the selectivity used and evaluates significance. Respect for copyright and intellectual property rights, and the correct usage of published material should be taught. Methods to detect plagiarism may need to be further developed and are certainly part of examination boards' thinking.

Possible statements:

- K** If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider via the ICT co-ordinator.
- K** Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

The following statements require adaptation according to the pupils' age:

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

2.3 Managing Information Services

2.3.1 How will information systems security be maintained?

Discussion: It is important to review the security of the whole system from user to Internet service provider (ISP). This is a major responsibility that includes delivery of essential services to the personal safety of staff and pupils.

ICT security is a complex matter and cannot be dealt with adequately in this document. A number of agencies can advise on security including Becta, EIS and suppliers. The Schools ICT Security Policy www.eiskent.co.uk (**broadband link**) provides further information and discussion.

Local Area Network security issues include:

- Users must act reasonably – the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for network use. For KCC staff, disregarding ICT usage policy is regarded as a matter for dismissal.
- Workstations should be secure from mistakes by the user.
- Servers must be located securely and physical access restricted.
- The server operating system must be secure and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be pro-actively managed.

Wide Area Network (WAN) security issues include:

- All Internet connections must be achieved via the Kent Community Network to ensure compliance with the security policy.
- KCN firewalls and switches are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership basis between school and KCN.

The Kent Community Network includes a cluster of Nokia appliances at each of the Internet connecting nodes. These appliances run the industry-standard CheckPoint firewall 1 system. The firewalls are maintained by the Unisys Security Centre.

Possible statements:

- K** The security of the school information systems will be reviewed regularly.
- K** Virus protection will be installed and updated regularly.
- K** Security strategies will be discussed with the LA.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not be used without specific permission and a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The IT co-ordinator / network manager will review system capacity regularly.

2.3.2 How will e-mail be managed?

Discussion: E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between neighbouring villages and even continents can be created.

The implications of e-mail use for the school and pupils need to be thought out and appropriate safety measures put in place. Un-regulated e-mail can provide routes to pupils that bypass the traditional school boundaries.

A central question is the degree of responsibility that can be delegated to individual pupils. Once e-mail is available it is difficult to control. Restriction of incoming and outgoing e-mail to approved addresses and filtering for unsuitable content and viruses is now possible.

In the school context, e-mail should not be considered private and most schools and many firms reserve the right to monitor e-mail. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

The use of e-mail identities such as **john.smith@school.kent.sch.uk** needs to be considered, as individual pupils email accounts could be predicted. For primary schools, whole-class or project e-mail addresses are easy to use and monitor. E-mail accounts such as **John234@school.kent.sch.uk** might be considered safer for younger secondary pupils, although confusion between pupils will be increased. Yet more anonymous, and confusing, would be **Jane4567@kent.sch.uk**. Older pupils and staff may continue to prefer the full name convention and can manage any issues that may arise.

Many teenagers have their own e-mail accounts, such as the web-based Hotmail, which they use widely outside school. Most schools ban access to external web-based email, particularly as anonymous identities such as **pjb354@mailhost.com** make monitoring difficult. Strategies include limiting pupils to e-mail accounts on the school domain or restricting e-mail traffic to the school domain.

Much e-mail use is purely of a social nature. Is social e-mail use considered to be useful experience of a communications tool or is it judged as low priority? Should access to social e-mail only be made available outside lesson hours?

Spam, phishing and virus attachment can make email dangerous. The Kent Community Network uses IronPort email relays to stop unsuitable mail using reputation filtering, currently about 95% is rejected.

Possible statements:

- K** Pupils may only use approved e-mail accounts on the school system.
- K** Pupils must immediately tell a teacher if they receive offensive e-mail.
- K** Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- K** Whole-class or group e-mail addresses should be used in primary schools.
 - Access in school to external personal e-mail accounts may be blocked.
 - Excessive social e-mail use can interfere with learning and may be restricted.
 - E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
 - The forwarding of chain letters is not permitted.

2.3.3 How will published content be managed?

Discussion: Many schools have created excellent Web sites that inspire pupils to publish work of a high standard. Web sites can celebrate pupils' work, promote the school and publish resources for projects or homework. Editorial guidance will ensure that the Web site reflects the school's ethos, that information is accurate, the site is well presented and that personal security is not compromised. Common values and quality control should be shared between Web and paper publication.

Information about schools and pupils could be found from a newsletter but a school's Web site can be accessed by anyone. Publication of information should be considered from a security viewpoint. Material such as staff details or a detailed plan of the school may be better published in the school handbook or on an intranet and thereby restricted to known persons. Secure access to parts of a school website by authorised people such as parents is an important development.

Possible statements:

- K** The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- Email addresses should be published carefully, to avoid spam harvesting.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

2.3.4 Can pupil's images or work be published?

Discussion: Photographs that include pupils add a liveliness and interest to a Web site or blog that is difficult to achieve in any other way. Nevertheless the security of staff and pupils must come first. Sadly, although common in newspapers, the publishing of pupils' names with their photographs is not acceptable. Web images could be misused and individual pupils identified unless broad descriptions are used.

Strategies include using relatively small photographs of groups of pupils and using photographs that do not show faces at all. "Over the shoulder" can replace "passport-style" photographs but still convey the educational activity and personal photographs can be replaced with self-portraits or images of pupils' work or of an activity. A check should be made that pupils in photographs are appropriately clothed.

Photographs of a pupil should not be published without the parent's or carer's written permission. Some schools ask for permission to publish images of work or appropriately taken photographs of pupils once per year, others at the time of use.

Pupils also need to be taught the reasons for caution in publishing personal information and photographs in social publishing sites (see section 2.3.6).

Possible statements:

- K** Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- K** Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- K** Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.

2.3.5 How will social networking and personal publishing be managed?

Discussion: Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: blogs, wikis, MySpace, Bebo, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

Possible statements:

- K** Schools should block/filter access to social networking sites.
- K** Newsgroups will be blocked unless a specific use is approved.
- K** Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name, school or shopping centre.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for students on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

2.3.6 How will filtering be managed?

Discussion: Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community. Older secondary pupils, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. Systems to adapt the access profile to the pupil's age and maturity are available.

The technical strategies being developed to restrict access to inappropriate material fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled-garden or allow list provides access only to a list of approved sites. Such lists inevitably restrict pupils' access to a narrow range of information.
- Dynamic filtering examines the content of Web pages or e-mail for unsuitable words. Filtering of outgoing information such as Web searches is also required.
- Rating systems give each Web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
- Access monitoring records the Internet sites visited by individual users. Access to a site forbidden by the filtering policy will result in a report.

Schools installing their own filtering systems are taking on a great deal of responsibility. Hundreds of inappropriate sites are created each day and many change URLs to confuse filtering systems. Management time will be considerable.

The Kent Community Network uses Websense which is an industry-standard system used by a many local authorities across the UK. Secondary schools have their own filtering server and manage their own filtering policy. Primary schools use area-based Websense servers with a rapid response from KCN staff if changes are required.

Possible statements:

- K** The school will work in partnership with the LA, Becta and the Internet Service Provider to ensure filtering systems are as effective as possible.
- K** If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the internet service provider.
- Larger schools, generally secondary, will manage the configuration of their filtering. This task requires both educational and technical experience.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP (addresses later).
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

2.3.7 How will videoconferencing be managed?

Discussion: Videoconferencing enables users to see and hear each other between different locations. It is a 'real time' interactive technology and has many uses in education.

Equipment ranges from small PC systems (web cameras) to large room based systems that can be used for whole classes or lectures. The videoconferencing equipment uses a 'network' to communicate with the other site.

Currently, two main types of network environments are used in videoconferencing: ISDN circuit connections and more recently IP (Internet Protocol) networks.

The traditional method has been to use ISDN (Integrated Services Digital Network) which provides a direct connection over a dial up service. Each videoconferencing system has a unique ISDN number, like a telephone number. One disadvantage of this network is that it is expensive to run. ISDN may be the only choice where access to broadband IP connectivity is not available, or where the distant school only has ISDN (although IP / ISDN gateways are available).

Videoconferencing has recently developed over IP networks. All modern standards-based videoconferencing systems will connect over IP. Videoconferencing over the Internet, even with a broadband connection, is unpredictable since it is a shared network and quality of service cannot be controlled. Schools using the Internet for videoconferencing should be aware that it is not managed by a single responsible agency and that there is no inherent security.

Recently the National Educational Network (NEN) has been developed. This is a secure, broadband, IP network interconnecting the ten regional schools networks across England with the Welsh, Scottish and soon the Northern Irish networks. Schools can thus use IP technology in a secure and managed environment.

Schools with full 'DfES Specification' broadband are connected through the LA and Regional Broadband Consortia and have access to services such as gatekeepers and gateways to enable schools to communicate with other locations outside their LA. MCUs (Multipoint Control Units) enable several schools to communicate at one time, for instance with several video streams each in a screen window.

Possible statements:

The equipment and network

- K** All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- K** IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- K** Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- K** External IP addresses should not be made available to other sites.
 - Videoconferencing contact information should not be put on the school web site.
 - The equipment must be secure and if necessary locked away when not in use.
 - School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

DRAFT for COMMENT

Users

- K** Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- K** Videoconferencing should be supervised appropriately for the pupils' age.
 - Parents and Guardians should agree for their children to take part in videoconferences, probably in the annual return.
 - Responsibility for the use of the videoconferencing equipment outside school time needs to be established with care.
 - Only key administrators should be given access to the videoconferencing system web or other remote control page available on larger systems.
 - Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- K** When recording a lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- K** Recorded material shall be stored securely.
- K** If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).
 - Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
 - Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

2.3.8 How can emerging technologies be managed?

Discussion: Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia. A risk assessment needs to be undertaken on each new technology and effective practice in classroom use developed. The safest approach is to deny access until a risk assessment has been completed and safety demonstrated.

For many schools email should be considered an emerging technology. E-mail can be sufficient to set up a virtual community. The pupils in two schools could create a shared project using class e-mail and a common Web site or blog. Staff and governors make a larger community, which could be extended to include parents.

Virtual classrooms and virtual communities widen the geographical boundaries of learning. New approaches such as mentoring and parent access to assessment scores are being investigated. Is an on-line community one way to encourage a disaffected pupil to keep in touch?

The safety and effectiveness of wider virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites such as Bebo. The registering of individuals to establish and maintain validated electronic identities is an important part of the process.

Video conferencing introduces new dimensions. Web cameras cost as little as £50 and, with faster Internet access, can enable limited video to be exchanged across the Internet. The availability of live video can increase safety – you can see who you are talking to – but if inappropriately used, a video link could reveal security details.

New applications are continually being developed based on the Internet, the mobile phone network, wireless or infrared connections. Users can be mobile using a phone or personal digital assistant with wireless Internet access. Should a pupil be allowed to use a phone to video a teacher's annoyed reactions in a difficult situation?

Schools should keep up to date with new technologies, including those relating to mobile phones and hand-held devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many pupils. Could teachers communicate with a truanting pupil? Could reminders for exam coursework be sent by text message? There are dangers for staff if personal phones are used to contact pupils and a school owned phone might be issued.

The inclusion of inappropriate language or graphical icons within text messages is difficult for staff to detect. Pupils may need reminding that such usage is both inappropriate and conflicts with school policy. Abusive text messages would be dealt with under the school bullying policy.

Possible statements:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- The school should investigate cellular wireless, infra-red and Bluetooth communication and decide a policy on phone use in school.
- Staff will be issued with a school phone where contact with pupils is required.

DRAFT for COMMENT

2.3.9 How should personal data be protected?

Discussion: The quantity and variety of data held on pupils, families and on staff is expanding quite quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify an individual). The act also gives rights to the people the information is about i.e. the right of subject access, lets individuals find out what information is held about them.

The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individuals rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Schools will already have information about their obligations under the Act, and this section is a reminder that all data in which people can be identified is protected.

For advice and guidance relating to a contravention of the Data Protection Act 1998, contact Michelle Hunt:

Access to Information Co-ordinator
Communication & Information Governance
Children, Families & Education Directorate
Kent County Council
Sessions House
Email: michelle.hunt@kent.gov.uk Tel: 01622 696692

The Kent Data Protection information may be seen at:
http://www.clusterweb.org.uk/Policy/dpfoi_data.cfm

Information Commissioner's Office:
<http://www.ico.gov.uk/>

Possible statements:

- K** Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.4 Policy Decisions

2.4.1 How will Internet access be authorised?

Discussion: The school should allocate Internet access for staff and pupils on the basis of educational need. It should be clear who has Internet access and who has not. Authorisation is generally on an individual basis in a secondary school. In a primary school, where pupil usage is fully supervised, all pupils in a class could be authorised as a group. As most pupils will be granted Internet access, it may be easier to manage lists of those who are denied access. Parental permission will be required in all cases - a chore that may be best organised annually when pupils' home details are checked.

Possible statements:

- K** The school will maintain a current record of all staff and pupils who are granted Internet access.
- K** All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- K** At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised Internet access (an example letter for primary schools is available).
- Secondary students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.
- Parents will be asked to sign and return a consent form for pupil access.

2.4.2 How will risks be assessed?

Discussion: As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will need to address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system. It is wise to include a disclaimer such as the following.

Possible statements:

- K** In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

2.4.3 How will e-safety complaints be handled?

Discussion: Parents, teachers and pupils should know how to submit a complaint. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school.

A minor transgression of the rules may be dealt with by the teacher. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator or e-Safety coordinator. Advice on dealing with illegal use could be discussed with the local Police Youth Crime Reduction Officer.

See also section **1.9 Response to an incident of concern.**

Possible statements:

- K** Complaints of Internet misuse will be dealt with by a senior member of staff.
- K** Any complaint about staff misuse must be referred to the headteacher.
 - Pupils and parents will be informed of the complaints procedure.
 - Parents and pupils will need to work in partnership with staff to resolve issues.
 - Discussions will be held with the local Police Youth Crime Reduction Officer liaison officer to establish procedures for handling potentially illegal issues.
 - Sanctions within the school discipline policy include:
 - interview/counselling by head of year;
 - informing parents or carers;
 - removal of Internet or computer access for a period.

2.4.4 How is the Internet used across the community?

Discussion: The Internet is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, supermarket or cyber café. Ideally, young people would encounter a consistent policy to Internet use wherever they are.

In community Internet access there is a fine balance to be achieved in ensuring 'freedom of information' whilst providing adequate protection for children and others who may be offended by inappropriate material. Each organisation is developing access appropriate to its own client groups and pupils may find variations in the rules and even unrestricted Internet access. Although policies and practices may differ, community partners adhere to the same laws as schools with respect to content, copyright and misuse. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with pupils on the reasons for the differences could be worthwhile.

Sensitive handling of cultural aspects is important. For instance filtering software should work across community languages and school Internet policies may need to reflect the pupils' cultural backgrounds. Assistance from the community in drawing up the policy could be helpful.

Possible statements:

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

2.5 Communications Policy

2.5.1 How will the policy be introduced to pupils?

Discussion: Many pupils are very familiar with Internet use and culture and it might be wise to discuss or design the School e-Safety Policy with them, possibly through a student council. As pupils' perceptions of the risks will vary, the rules for responsible use may need explanation and discussion. Pupils may need to be reminded of the school rules, possibly by posters at the point of Internet use.

Later in this document 'Responsible Internet Use' rules are suggested, with versions as posters for KS1, KS2 and secondary pupils and for staff. A copy could also be given to parents when they are asked to consent to Internet use. Consideration must be given as to the curriculum place for e-safety, is it an ICT activity, part of the pastoral programme or part of every subject?

Useful e-safety programmes include:

- Think U Know; currently available for secondary pupils. (www.thinkuknow.co.uk/)
- SuperClubs (ex. GridClub) www.superclubsplus.com/
- The BBC's ChatGuide: www.bbc.co.uk/chatguide/

Possible statements:

- K** Rules for Internet access will be posted in all networked rooms.
- K** Pupils will be informed that Internet use will be monitored.
- An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- A module on responsible Internet use will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

2.5.2 How will the policy be discussed with staff?

Discussion: It is important that all staff feel confident to use the Internet in teaching. The School e-Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

Staff must understand that the Internet misuse rules for KCC employees are quite specific. Instances of misuse resulting in dismissal have occurred. If a member of staff is concerned about any aspect of their Internet use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

Internet use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. The induction of new staff should discuss Internet issues, for instance the selection of appropriate modes of expression in e-mail communication to prevent confusion.

DRAFT for COMMENT

Possible statements:

- K** All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
 - Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
 - Staff development in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

2.5.3 How will parents' support be enlisted?

Discussion: Internet use in pupils' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate, supervised use of the Internet at home. Parents should also be advised to check if pupils' use elsewhere is covered by an appropriate use policy. One strategy is to help parents to understand more about ICT - perhaps by running courses (although the resource implications will need to be considered).

Possible statements:

- K** Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- Internet issues will be handled sensitively to inform parents without alarm.
 - A partnership approach with parents will be encouraged. This could include parents evenings with demonstrations and suggestions for safe home Internet use.
 - Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
 - Interested parents will be referred to organisations listed in section 4.0 e-Safety Contacts and References.

3.0 Supporting materials

Responsible Use Posters for KS1, KS2 and secondary.

Printed copies of posters are available at A4 and A3 size without charge from:

EIS, Oxford Road, Maidstone, Kent ME15 8AW.

Please send a stamped, self-addressed envelope (A4 large).

Sample letter to parents – primary

Sample permission form.

Sample Acceptable ICT Use Agreement for staff.

All materials are available from the e-safety website:

<http://www.clusterweb.org.uk?esafety>

4.0 e-Safety Contacts and References

CFE e-Safety Officer,
KCC Children Families & Education
Rebecca Chapman
e-mail: rebecca.chapman@kent.gov.uk
Tel No: 01622 696590

Children's Officer for Training & Development,
Child Protection
Mike O'Connell
E-mail: mike.oconnell@kent.gov.uk
Tel No: 01622 696677

Kent Community Network HelpDesk
Help with filtering and network security. 01622 206040

Schools ICT Security Policy
<http://www.eiskent.co.uk> (broadband link)

e-Safety in Schools and Schools e-Safety Policy
<http://www.clusterweb.org.uk?esafety>

Schools e-Safety Blog
<http://clusterweb.org.uk?esafetyblog>

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk/contact_us.html

Virtual Global Taskforce – Report Abuse
<http://www.virtualglobaltaskforce.com/>

Think U Know website
<http://www.thinkuknow.co.uk/>

Becta
<http://www.becta.org.uk/schools/esafety>

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

Internet Safety Zone
<http://www.internetsafetyzone.com/>

Kidsmart
<http://www.kidsmart.org.uk/>

NSPCC
<http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm>

Childline
<http://www.childline.org.uk/>

Stop Text Bully
www.stoptextbully.com

NCH – The Children's Charity
<http://www.nch.org.uk/stories/index.php?i=324>

NCH – Digital Manifesto
http://www.nch.org.uk/uploads/documents/Digital_Manifesto_web.pdf

BBC Chat Guide
<http://www.bbc.co.uk/chatguide/>

5.0 Acknowledgements

This edition has been the work of:

Peter Banbury EIS, Mandy Barrow, ASK; Martin Carter, Kent Police; Rebecca Chapman, CFE; Alan Day, CFE; Alison Gaunt, ASK; Rachel Keen, SENICT; Steve Moores, Maidstone Grammar; Mike O'Connell, CFE Child Protection; Sarah Quantick, ASK / The Community College Whitstable; Helen Smith, ASK; Marc Turner, EIS and Carol Webb, Invicta Grammar.

The five previous editions involved a very wide group of people including Kent teachers and officers, SEGfL, NAACE and the British Computer Society Expert Schools Panel.

John Allen, ASK; Steve Bacon, NAACE; Clive Bonner, EIS; Ian Coulson, ASK; Sandra Crapper, Consultant; Kevin Figg, Westlands; Maureen Gillham, Weald of Kent Grammar; Michael Headley, EIS; Greg Hill, SEGfL; Andrew Lamb, Whitfield Primary; Paul Newton, Kent NGfL; Richard Packham, EIS; Ian Price, Child Protection; Sandra Patrick, Kent NGfL; Tom Phillips, KCC; Graham Read, Simon Langton Girls Grammar; Martin Smith, Highsted Grammar; Chris Shaw, EIS; Linda Shaw, Kent NGfL; Chris Smith, Hong Kong; John Smith, Wakefield LEA; Helen Smith, Kent NGfL; Laurie Thomas, KCC; Clare Usher, Hugh Christie; Gita Vyas, Northfleet School for Girls; Carol Webb, Invicta; Ted Wilcox, Borden Grammar. Roger Blamire, BECTa; Stephanie Brivio, Libraries; Les Craggs, KAS; Alastair Fielden, Valence School; John Fulton, Hartsdown; Keith Gillett, Seal Primary; Doreen Hunter, Deanwood Primary Technology School; Steve Murphy, Drapers Mills Primary; Judy Revell, KCC; Chris Ridgeway, Invicta Grammar; Nick Roberts, Sussex LEA; Graham Stabbs, St Margarets at Cliffe Primary; Sharon Sperling, KCC; Brian Tayler, KCC; Joanna Wainwright, KCC; Richard Ward, KCC; Theresa Warford, Libraries; Ian Whyte, Plaxtol Primary; Chris Woodley, KCC; Heather Pettitt, SEGfL; Ian White, SWGfL; Greg Hill, SEGfL.

ASK is the Advisory Service for Kent. SEGfL is the South East Grid for Learning.

6.0 Notes on the legal framework

An awareness of legal issues is important, but this page is not definitive advice.

Many young people and indeed some staff use the internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes include:

- The 2003 Sexual offences Act has introduced new offences of Grooming and raised the age for making/distributing indecent images of children to 18.
- Offences regarding racial hatred are covered by the Public Order Act 1986 although a new Racial and religious Hatred Bill is going through parliament.

6.1 Possible offences:

Sexual Offences Act 2003

- Grooming – If you are over 18 and have communicated with a child under 16 at least twice (including by phone or internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.
- Making indecent images – it is an offence to take, make, distribute, show, advertise indecent images of a child under 18. (NB to view an indecent image on your computer means that you have made a digital image.)
- Causing a child under 16 to watch a Sexual Act – to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.
- Abuse of positions of trust - Staff must be aware that it is an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Applies to teachers, social workers, health professionals, connexions staff)

N.B. Schools should already have a copy of 'Children & Families: Safer from Sexual Crime' document as part of their child protection packs.

Information about the 2003 Sexual Offences Act can be found at www.teachernet.gov.uk

6.2 Relevant Legislation

The Computer Misuse Act 1990 - makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Public Order Act 1986 – offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

Communications Act 2003 - There are 2 separate offences under this act:

- a. sending by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.
- b. sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.

DRAFT for COMMENT

This wording is important because the offence under a. is complete when the message has been sent - no need to prove any intent or purpose. It is an offence under b. to keep using the network for sending any kind of message irrespective of content if for the purpose of causing annoyance etc.

Malicious Communications Act 1988 – offence to send a letter, electronic communication or article which is indecent or grossly offensive, threatening or false information with intent to cause distress or anxiety to the recipient.

Copyright, Design and Patents Act 1988 - it is an offence to use unlicensed software

Protection of Children Act 1978 - The law on images of child abuse is clear. It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom.

Obscene Publications Act 1959 and 1964 - defines “obscene” and related offences.

Protection from Harassment Act 1997

Section 2 - A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

Section 4 - A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

6.3 Monitoring School ICT Use

Monitoring network activity could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998.

The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day to day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Schools could start by banning private use of the network, but then allow private use following application to the head teacher. The Rules for Responsible Internet Use, with which every user agrees to comply, contains a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring.

6.4 Sex Offences Act 2003 Memorandum of Understanding

Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003

The aim of this memorandum is to help clarify the position of those professionally involved in the management, operation or use of electronic communications networks and services who may face jeopardy for criminal offences so that they will be reassured of protection where they are acting to combat the creation and distribution of images of child abuse. This memorandum has been created within the context of child protection, which will always take primacy.

The MOU: <http://www.iwf.org.uk/police/page.22.213.htm>