

BucksGfL e-Safety Guidance for schools

May 2007

Buckinghamshire County Council believes that the use of information and communication technologies in schools brings great benefits. Recognising the e-safety issues and planning accordingly will help to ensure appropriate, effective and safe use of electronic communications. This guidance and policy template will help schools to discuss the issues and review their e-Safety Policy

Schools e-Safety Policy Guidance

Executive Summary

The use of information and communication technologies (ICT) including the Internet has developed over the past 25 years and now involves every pupil and member of staff. Such powerful technologies have their dangers and society is still struggling to react adequately to the issues raised.

However we need to recognise that not all schools have a current and considered policy, not all staff are fully aware of online risks and that few schools teach e-safety adequately. We ask schools to turn policy into effective practice.

Meanwhile pupils are way ahead of us with social networking, instant messaging, text and mobile use although many young people lack an appreciation of online dangers and of the consequences of their actions.

Please make e-safety a priority.

Disclaimer

Buckinghamshire County Council (BCC) makes every effort to ensure that the information in this document is accurate and up-to-date.

If errors are brought to our attention, we will correct them as soon as practicable.

Nevertheless, BCC and its employees cannot accept responsibility for any loss, damage or inconvenience caused as a result of reliance on any content in this publication.



CONTENTS

1. Schools' e-Safety Policy Guidance

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

2. Schools' e-Safety Policy Template

- 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 be used across the community?
- 2.5 Communicating the 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 e-Safety Contacts and References

4.0 Acknowledgments

5.0 Legal Framework

Supporting Materials are published on www.bucksgfl.org.uk and www.bucksict.org.uk

Schools e-Safety Policy Guidance

1.1 Why write an e-safety policy?

Pupils interact with new technologies such as mobile phones and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are 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, critical and responsible ICT use wherever the young people may be.

This guidance document has been produced to inform the e-safety debate and to help schools write their own e-safety policies. The policy template provides a range of statements to make policy review easier and more comprehensive.

E-safety covers issues relating to children and young people and their safe use of the Internet, mobile phones and other electronic communications 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) and detailed materials for schools are available from Becta.

1.2 What is e-safety?

The School's e-Safety Policy should update and replace its Internet 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. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally 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 access to which access would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others.

Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to 'groom' children.

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 and measures put in place 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. The policy template provides a structure for policy writing and material to stimulate this essential debate.

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 modify or replace any statement.

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 may already be out of date.

1.4 Responsibilities of school staff

Information technologies are developing rapidly and can leave staff unsure of best practice or how to discuss e-safety issues with pupils. Advice and training may be obtained from the BucksICT Curriculum support team, the ICT adviser or BucksCC child protection officers.

The trust between pupils and school staff is essential to education but very occasionally it can break down. This is not new, but has been highlighted by better awareness of human failings and greater respect for children. Nationally, CEOP has been set up by the Home Office to “safeguard children’s online experiences and relentlessly track down and prosecute offenders”.

In school as in industry, a member of staff who flouts security advice, or uses e-mail or the Internet for inappropriate reasons risks dismissal.

All staff should sign an information systems code of conduct on appointment. Staff will thereby accept that the school can monitor network and Internet use to help ensure staff and pupil safety.

Staff that manage filtering systems or monitor ICT use have great responsibility and must be appropriately supervised. 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 essential reading.

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

E-mail, text messaging and IM all provide additional channels of communication between staff and pupils and inappropriate behaviour can occur, or communications can be misinterpreted. Staff might reflect on the power of the technology in Police hands to identify the sender of inappropriate messages. Some schools are providing phones for staff-pupil contact to protect staff from false accusations.

1.5 Routes to e-safety - primary pupils

A very present danger

Despite precautions at school, open access to the Internet has become an integral part of many children’s lives. A growing danger is presented by the ease of uploading material to the Web. We already have evidence from 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 are very limited 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. Children who have poor social skills may be more at risk from inappropriate online contact.

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 Internet 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 the image or window 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 and 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 generally online at all times when a user is logged on.

Web Link

- **Signposts to Safety**, Key Stage 1 + 2 version, Becta (April 2007)
- <http://publications.becta.org.uk>

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 download them, as long as an adult downloads the 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/>

While tagged image browsers are fun to explore (a good example is www.airtightinteractive.com/projects/related_tag_browser/) There is a danger is that this will accept inappropriate keywords. While useful to teachers, we can not recommend it for use by pupils. Links such as this must not be stored in the 'Favorites' folder 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').

The web filtering system used within BucksGfL is very powerful. However, please note that NO filtering engine is completely safe.

The homepage in many BucksCC 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 can be readily found on an unfiltered network. A far better starting point is RM **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. 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/e-mail/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!

E-mail

Within BucksGfL an email service is provided that offers every student, teacher, administrator and manager their own email account in a format designed to support the DfES' recommendations of regional and personal anonymity, and conforms to an easily recognizable standard.

NB: Nominated Contacts: please keep your account and password details in a safe place. Ensure that someone else will have overall access to school e-mail accounts if you are on leave, absent or no longer working with the school.

Teaching e-Safety

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

Grid Club, set up by DfES, is now a subscription site, but hosts the Cyber Café, which is a free resource at http://www.gridclub.com/teachers/t_internet_safety.html. This e-safety teaching resource has won the Internet Watch Foundation Award for its 'contribution to a safer Internet' and is remarkably easy for pupils to use.

The BBC Chat Guide site <http://www.bbc.co.uk/chatguide> contains a range of carefully designed teaching packs for KS2 and KS3. There are games and advice for children and young people and a downloadable ChatGuide booklet for parents.

1.6 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 a range of issues when teaching e-safety but some common difficulties may be:

- They may still be 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 specialists and support staff.

This may take the form of child-focused strategies that would apply to a pupil with specific needs and would be made available to all staff involved 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.

1.7 Routes to e-safety – secondary pupils

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 issues:

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 little educational value. 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 may access the Internet 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.

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 should be matched to the age and curriculum requirements of the Student.

However, due to the international scale and connected 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's Internet access should be designed expressly for student use and will include filtering appropriate to the age of the student.

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

e-safety 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 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 author of the information used and to respect copyright when using Internet material in their own work.

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 a good 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 use abusive language in your messages to others.
- Do not reveal the 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 monitor and may have access to e-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 may come with Internet, Bluetooth and infrared (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
- Digital video

Some of these technologies may disappear, but some will change our world. What is important 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, Key Stage 3 + 4**, Ref: BEC1-15274

1.8 Response to an incident of concern

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

An e-Safety Policy should 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 others.

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 considered illegal activity.

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 Safeguarding Service or the Police if that becomes necessary.

What does electronic communication include?

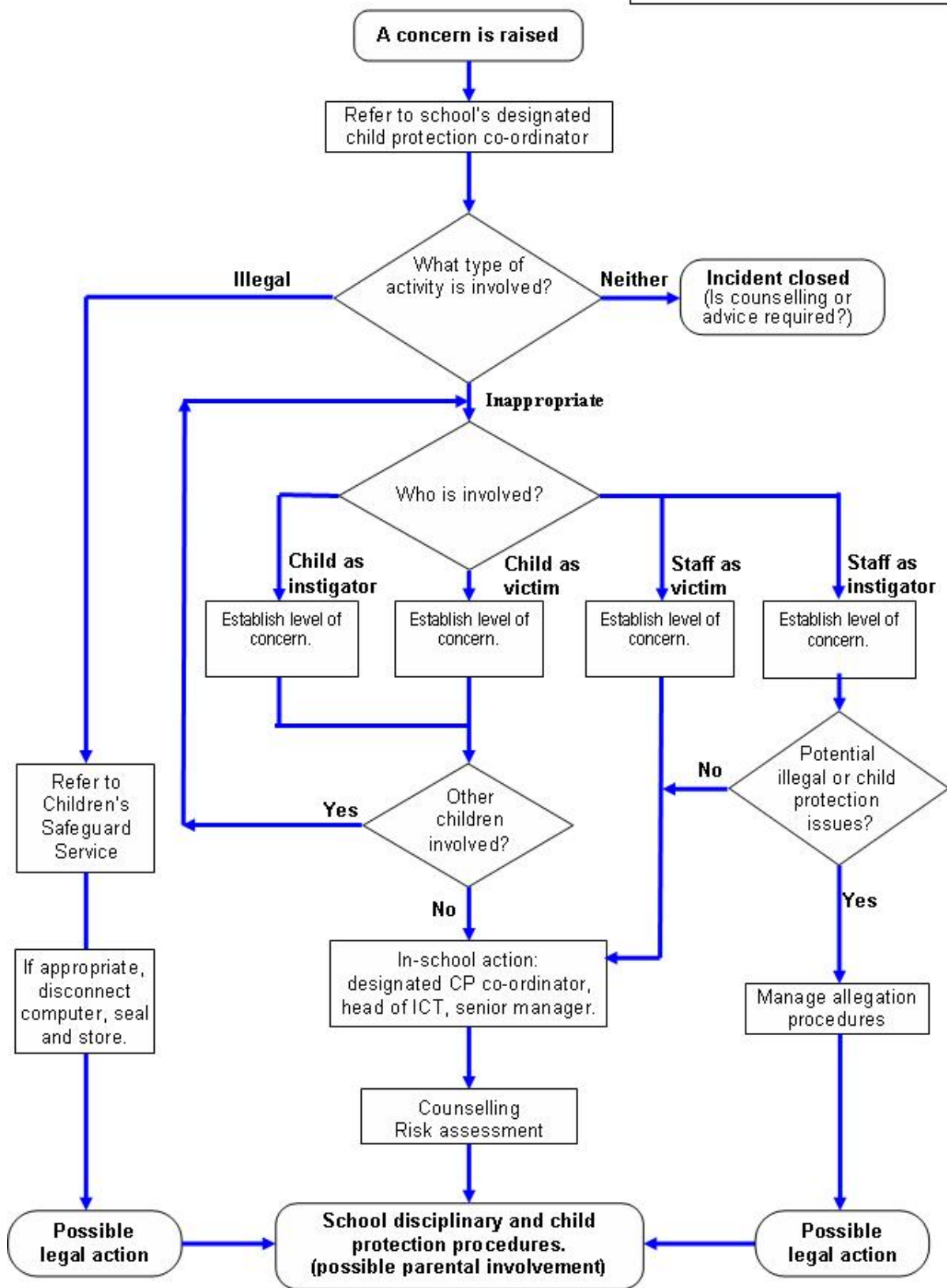
- **Internet collaboration tools:** social networking sites and web-logs (blogs)
- **Internet research:** websites, search engines and web browsers
- **Mobile phones and personal digital assistants (PDAs)**
- **Internet communications:** e-mail and IM
- **Webcams and videoconferencing**
- **Wireless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

What are the risks?

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

Response to an Incident of Concern

How do we respond?
 The flowchart below illustrates an approach to investigating such an incident.



1.10 School responsibilities

As e-Safety is a relatively new concept and covers a wider scope than Internet use. This list could assist a school in developing a co-ordinated and effective approach to managing e-Safety issues.

The following should be considered:

- BucksCC encourages schools to appoint an e-Safety Coordinator. 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. The e-Safety coordinator should maintain the e-Safety Policy, manage e-Safety training and keep abreast of local and national e-safety awareness campaigns.
- Schools should review their policy regularly and revise their policy annually to ensure that it is current and considers any emerging technologies.
- Schools should audit their filtering systems regularly to ensure that inappropriate websites are blocked.
- To ensure that pupils and staff are adhering to the policy, any incidents of possible misuse will need to be investigated.
- Schools should include e-Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupil need to know how to control and minimise online risks and how to report a problem.
- All staff must read and sign the school's e-Safety Code of Practice.
- Parents should sign and return the e-Safety Rules consent form.
- The e-Safety Policy should be made available to all staff, governors, parents and visitors.
- **Implementation and Compliance**
 - No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences. The following ideas and checks may be useful:
 - The quick audit provided in the Core e-Safety Policies is a good place to start when checking the schools e-safety readiness.
 - How are pupils reminded of their responsibilities? Displaying posters in rooms with computers is one useful approach.
 - Do staff, pupils and parents know how to report an incident of concern regarding Internet use?
 - Where filtering is managed locally, does a senior manager approve the school filtering configuration and supervise the staff who manage the filtering system?

2.0 School E-Safety Policy Template

Document format: In each of the paragraphs below a question invites discussion followed by recommended guidance statements for schools to use in the preparation of their e-Safety Policy.

Careful consideration of these is important as the statements cover a wide variety of situations and some may be inappropriate for your school. Naturally schools may edit the statements or substitute their own. Your feedback on statements will inform future editions.

2.1.1 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:

- The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on the BucksCC 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 and its implementation will be reviewed annually.

2.2 Teaching and learning

2.2.1 Why is Internet use important?

Discussion: The rapid developments in electronic communications are having many effects, some profound, on society. Only ten years ago we were asking whether the Internet should be used in all schools. Now every pupil is younger than 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 functions.
- 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 set a target that all schools should have broadband Internet use by 2006. Schools should have access to personal learning spaces by 2008 and learning platforms by 2010. A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet.

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 BucksCC and the 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 learning outcomes must also be addressed. Developing effective practice in Internet use for teaching and learning is essential. Librarians and teachers can help pupils to learn how to distil the meaning from the mass of information provided by the Internet. Often the quantity of information is overwhelming and staff may guide pupils to appropriate websites, or teach search skills. Offering younger pupils a few good sites is often more effective than an Internet search. Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet.

Possible statements:

- The school's Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- 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 Internet, e-mail or text message requires good 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 Internet, 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.

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. BucksGfL 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 use 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:

- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and 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 Systems

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. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils. ICT security is a complex matter and cannot be dealt with adequately in this document.

Local Area Network security issues include:

- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For BucksCC staff, flouting electronic use policy is regarded as a matter for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured 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 should be arranged via the BucksGfL to ensure compliance with the security policy.
- BucksGfL firewalls and switches are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership basis between school and BucksCC.

Possible statements:

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with BucksCC advisers.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not be used without specific permission followed by 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 ICT 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 schools in neighbouring villages and in different continents can be created.

The implications of e-mail use for the school and pupils need to be thought through 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 unrestricted e-mail is available it is difficult to control. Spam, phishing and virus attachment can make e-mail dangerous but filtering for unsuitable content and viruses in email is now available through BucksGfL.

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.

BucksGfL e-mail accounts such as **Jsmit234@bucksgfl.org.uk** is the standard format used for pupils. Many teenagers have their own e-mail accounts, such as the web-based Hotmail, which they use widely outside school. BucksGfL normally bans access to external web-based e-mail, particularly as anonymous identities such as **pjb354@mailhost.com** make monitoring difficult.

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?

Possible statements:

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- 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 websites that inspire pupils to publish work of a high standard. Websites can celebrate pupils' work, promote the school and publish resources for projects. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

Sensitive information about schools and pupils could be found from a newsletter but a school's website is more widely available. Publication of information should be considered from a personal and school security viewpoint. Material such as staff lists or a school plan may be better published in the school handbook or on a secure part of the website which requires authentication.

Possible statements:

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- E-mail addresses should be published carefully, to avoid spam harvesting.
 - The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
 - The website 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: Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. Sadly, although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be re-used, particularly if large images of individual pupils are shown.

Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport-style" photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed.

Images of a pupil should not be published without the parent's or carer's written permission. Some schools ask permission to publish images of work or appropriate personal photographs once per year, other schools ask at the time of use.

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

Possible statements:

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.
- 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, over which there may be limited control.

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:

- The schools will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full 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 or school.
- 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 student use 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 Internet 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 through BucksGfL.

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" restricts access to a list of approved sites. Such lists inevitably limit pupils' access to a narrow range of information.
- Dynamic filtering examines web page content 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. Attempted access to a site forbidden by the policy will result in a report.
- Key loggers record all text sent by a workstation and analyse it for patterns, often returning false positives requiring manual intervention.

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

The BucksGfL network uses **WebScreen**™ which is an industry-standard system used by a many local authorities. Some schools not using BucksGfL might have their own filtering server and manage their own filtering policy but this might be considered to be a high risk activity, requiring both educational and technical experience.

Possible statements:

- The school will work with BucksCC and BucksGfL to ensure that systems to protect pupils are regularly reviewed.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator.
- 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).
- The school's filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by BucksGfL.

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.

Two main types of network environments have been used in videoconferencing: ISDN circuit connections and more recently IP (Internet Protocol) networks.

Initially ISDN (Integrated Services Digital Network) was used, which provides a direct connection over a dial up service. However ISDN will shortly be discontinued by BT.

Videoconferencing now uses IP networks. All modern standards-based videoconferencing systems will connect over IP. However, videoconferencing over the Internet, even with a broadband connection, can sometimes be unpredictable since it is a shared network and quality of service cannot always be controlled. Schools using the publicly available software such as 'Skype' over 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 the Northern Ireland networks. Within this schools can now use IP technology in a secure and managed environment.

Schools with full 'DfES Specification' broadband are connected through the BucksGfL Network and have access to services such as 'Adobe Connect' to enable schools to communicate with other schools within the NEN and also to external locations.

Possible statements:

The equipment and network

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- All videoconferencing equipment in the classroom must be switched off when not in use.
- Equipment connected to the educational broadband network should use the 'Adobe Connect' system or the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
 - Videoconferencing contact information should not be put on the school Website.
 - 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.
- Users
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- 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

- When recording a videoconference lesson, 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.
- Recorded material shall be stored securely.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- 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.

Even e-mail should be considered an emerging technology until rules have been set. 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 website 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 £10 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 images within text messages is difficult for staff to detect. Pupils may need reminding that such use is both inappropriate and conflicts with school policy. Abusive text messages may 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 wireless, infra-red and Bluetooth communication technologies and decide a policy on phone use in school.
- Staff will be issued with a school phone where contact with pupils is required.

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 quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 (“the 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 a living individual). The Act also gives rights to the people the information is about i.e. subject access rights 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 from which people can be identified is protected.

For advice and guidance relating to a contravention of the Act please contact the BucksCC data protection officer, further information is also available from the Information Commissioner's Office:

<http://www.ico.gov.uk/>

Possible statement:

- 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 task that may be best organised annually when pupils' home details are checked.

Possible statements:

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the 'e-safety Code of Conduct' before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Secondary students must apply for Internet access individually by agreeing to comply with the e-Safety Rules.
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised Internet access.

2.4.2 How will risks be assessed?

Discussion: As the quantity and breadth of 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, an example of which is given below.

Possible statements:

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor BucksCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- 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.

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:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- 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 to establish procedures for handling potentially illegal issues.
- Sanctions within the school discipline policy include:
 - interview/counselling by the 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: Internet access 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 open access to 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. 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.

Communicating the Policy

2.4.5 How will the policy be introduced to pupils?

Discussion: Many pupils are very familiar with mobile and Internet use and culture and it might be wise to involve them in designing the School e-Safety Policy, possibly through a student council. As pupils' perceptions of the risks will vary; the e-safety rules may need to be explained or discussed.

A pupil and parent agreement form should be attached to a copy of the e-safety rules appropriate to the age of the pupil and circulated to every member of the school.

Consideration must be given as to the curriculum place for teaching e-safety. Is it an ICT lesson activity, part of the pastoral programme or part of every subject? Or all of these?

Useful e-safety programmes include:

- Think U Know; currently available for secondary pupils. (www.thinkuknow.co.uk/)
- Grid Club www.gridclub.com
- The BBC's ChatGuide: www.bbc.co.uk/chatguide/

Possible statements:

- E-Safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network and 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.
- An e-safety module will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

2.4.6 How will the policy be discussed with staff?

Discussion: It is important that all staff feel confident to use new technologies 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 rules for information systems misuse for BucksCC employees are quite specific. Instances resulting in dismissal could occur. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's e-Safety Policy.

Possible statements:

- All staff will be given the School e-Safety Policy and its application and 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 training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

2.4.7 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 their child's 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:

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent 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 3.0 e-Safety Contacts and References.

3.0 e-Safety Contacts and References

BucksICT Support Team Website

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

BucksGfL Website

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

BBC Chat Guide

<http://www.bbc.co.uk/chatguide/>

Becta

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

Childline

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

Child Exploitation & Online Protection Centre

<http://www.ceop.gov.uk>

Grid Club and the Cyber Cafe

<http://www.gridclub.com>

Internet Watch Foundation

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

Internet Safety Zone

<http://www.internetsafetyzone.com/>

Kidsmart

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

NCH – The Children’s Charity

<http://www.nch.org.uk/information/index.php?i=209>

NSPCC

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

Stop Text Bully

www.stoptextbully.com

Think U Know website

<http://www.thinkuknow.co.uk/>

Virtual Global Taskforce – Report Abuse

<http://www.virtualglobaltaskforce.com/>

4.0 Acknowledgements

This e-safety guidance is based in part on the publication “Schools e-safety policy 2007” by Kent County Council and we gratefully acknowledge their permission to use it in the production of this document.

5.0 Legal Framework

6. Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional 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 have been enacted through:

- ⊙ The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the a child to 18 years old;
- ⊙ The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and
- ⊙ The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the 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.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also 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. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Schools may already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection information.

More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- ⊙ gain access to computer files or software without permission (for example using someone else's password to access files);
- ⊙ gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- ⊙ impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

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.

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.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.