


Schools and Settings e-Safety Policy Guidance 2010

Kent 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 safer use of electronic communications. This guidance and the associated policy template will help schools to discuss the issues and review their e-Safety Policy.

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

Children, Families & Education

Kent County Council






Schools and Settings e-Safety Policy Guidance 2010

Eighth Edition

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. While these advances bring many benefits, such powerful technologies have their dangers and society is still struggling to react adequately to the issues raised.

The KCC Children, Families and Education Directorate (CFE) is working with the Kent Safeguarding Children Board (KSCB) with an e-Safety Strategy Group comprising Teachers, Officers, Advisers, Police and Child Protection Officers. The group advises on the safe and secure use of ICT in schools and encourages responsible use outside school. The Schools e-Safety Policy Guidance and linked materials are their work.

However we need to recognise that not all schools have an up-to-date policy, not all staff are fully aware of online risks and that there is mixed practice in schools on teaching e-Safety. We ask schools to turn policy into effective practice.

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

CFE strategies include this Policy Guidance, Local Children's Service Partnership-based e-Safety training and security developments within the Kent Public Service Network (KPSN). CFE also works with national initiatives including those of Becta and the Child Exploitation and Online Protection centre (CEOP).

The safety of children including e-Safety is an essential priority.

Grahame Ward
Director - Capital Programme & Infrastructure

Disclaimer

Kent County Council (KCC) 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, KCC and its employees cannot accept responsibility for any loss, damage or inconvenience caused as a result of reliance on any content in this publication.

With thanks to Unisys,
the prime contractor for the Kent Public Service Network
for sponsoring the printing of this booklet.






Schools and Settings e-Safety Policy Guidance 2010

Contents






1.1 Why write an e-Safety policy?

Pupils interact with new technologies such as mobile phones, games consoles 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 and other settings must decide on the right balance between controlling access, setting rules and educating students for responsible use. Parents, libraries, youth clubs and other settings must develop complementary strategies to ensure safe, consistent and responsible ICT use wherever young people may be.

Teachers and officers working with child protection officers and Kent Police have produced this guidance 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.

Core e-Safety policies approved by the CFE Directorate in conjunction with the Kent Safeguarding Children Board (KSCB) have been published for situations where time precludes the debate that would ideally take place.

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. This document takes into account the findings and recommendations from Dr Tanya Byron's 2008 report "Safer Children in a Digital World". It also incorporates work carried out by national agencies such as the Child Exploitation and Online Protection Centre (CEOP), Childnet International and Becta.

The e-Safety policy will help support and protect children, young people and staff when using technology.

We are pleased that many individual establishments and local authorities across the UK used previous editions of the Kent materials. This edition incorporates your feedback and further suggestions for improvements are always welcome.

The Kent e-Safety materials may be copied and adapted for non-commercial educational purposes only, always provided that KCC's copyright is acknowledged. Readers outside Kent are asked to email us when they use these materials

This document is suitable for all Schools and other educational settings (such as Pupil Referral Units, 14-19 settings and Hospital Schools etc) and we encourage all establishments to ensure that their e-Safety policy is fit for purpose and individualised for the context of each setting. For clarity we have used the terms 'school', 'pupils' and 'students' throughout the document, but please think about wider educational settings.

Peter Banbury
peter.banbury@kent.gov.uk

Rebecca Avery, e-Safety Officer
esafetyofficer@kent.gov.uk

www.kenttrustweb.org.uk?esafety

© KCC Children, Families and Education Directorate, January 2010.






1.2 What is e-Safety?

The School's e-Safety Policy reflects the importance it places on the safe use of information systems and electronic communications.

e-Safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- e-Safety concerns safeguarding children and young people in the digital world.
- e-Safety emphasises learning to understand and use new technologies in a positive way.
- e-Safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- e-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

The Internet is an unmanaged, open communications channel. The World Wide Web, email, blogs and social networks 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.

Some of the material on the Internet is published for an adult audience and can include violent and adult content. Information on weapons, crime and racism may also be unsuitable for children and young people to access. Pupils need to develop critical skills to evaluate online material and learn that publishing personal information could compromise their security and that of others. Schools have a duty of care to enable pupils to use on-line systems safely.

Schools need to protect themselves from legal challenge and ensure that staff work within the boundaries of professional behaviour. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use email, 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" and ensure an Acceptable Use Policy is in place. e-Safety training is an essential element of staff induction and part of an ongoing CPD programme. 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.

The rapid development and accessibility of the Internet and new technologies such as personal publishing and social networking means that e-Safety is an ever growing and changing area of interest and concern. The school's e-Safety policy must reflect this by keeping abreast of the vast changes taking place around us.

The school's e-Safety Policy must operate in conjunction with other school policies including Behaviour, Child Protection and Anti-Bullying. e-Safety must be built into the curriculum.






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 may modify or replace any statement.

Some schools may feel they do not have the expertise to write their own policy. CFE has also provided core policy statements for primary and secondary schools which can be edited relatively quickly for discussion and approval by managers and governors.

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

http://www.becta.org.uk/safeguarding.php

Schools should revise their 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.

The policy template can be found in a separate document at
www.kenttrustweb.org.uk?esafety *'Schools and Settings e-Safety Policy Template 2010'*

1.4 The Online e-Safety Policy Generator

The online policy generator is available at ***www.policy.e-safety.org.uk***

This interactive tool enables Schools to prepare their e-Safety policy online by selecting and amending statements from a bank.

All stakeholders should be actively involved in using this tool to collaboratively create an appropriate e-Safety policy for their establishment.

1.5 Statement of authority

This document has been written by the CFE and KSCB e-Safety Strategy Group to reflect effective practice, to raise issues and to point to sources of expert knowledge. Kent Police and the Children's Safeguards Service have contributed to this guidance. National agencies such as Becta, Childnet International and CEOP have been consulted and their materials referenced.

Through this guidance, the CFE Directorate is making a strong statement as to the precautions that it expects schools to take. Schools basing their e-Safety policies on CFE guidance will be able to demonstrate more easily that they have taken reasonable steps to protect their pupils.

KCC strongly recommends that guidance highlighted by the red **K** in the e-Safety Policy template is included and is rigorously implemented.

KCC schools have the immediate responsibility for e-Safety and must carefully consider the issues raised in this document. An e-Safety audit is recommended, possibly using external expertise, to help ensure that all reasonable steps have been taken. Please see the e-Safety site for an audit tool.

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






1.6 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 can be obtained from the CFE e-Safety officer, ASK advisers or 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 was set up by the Home Office to "safeguard children's online experiences and relentlessly track down and prosecute offenders" and their work should be acknowledged and built upon by schools.

In industry and indeed within KCC, a member of staff who flouts security advice or uses email or the Internet for inappropriate reasons risks dismissal.

All staff should sign an information systems' Code of Conduct or Acceptable Use Policy on appointment. Staff 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 the Senior Leadership Team. Staff must be aware of dangers to themselves in managing ICT use, for instance in viewing inappropriate images to investigate their source.

Any allegation of inappropriate behaviour must be reported to the Senior Leadership Team and investigated with care. Advice should be sought from the Children's Officer for Child Protection and/or Kent Police.

Email, text messaging, Social Networking and Instant Messaging (IM) all provide additional channels of communication between staff and pupils. Inappropriate behaviour can occur and communications can be misinterpreted. Staff should be aware of the power of the Police to identify the sender of inappropriate messages. Schools should provide establishment email accounts for all staff and also consider providing phones for staff-pupil contact to protect staff from false accusations.

Staff should be aware that students may be subject to cyberbullying via electronic methods of communication both in and out of schools. Head teachers should be aware that they have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site (Education and Inspections Act 2006)

School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy (Education and Inspections Act 2006). It must be noted that staff should not examine devices themselves but they should be handed to the Senior Leadership Team and potentially the police for investigation.






1.7 Routes to e-Safety — Primary pupils

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 Facebook, 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. It should be noted that most social networking and social media sites have age restrictions, typically 13+ and therefore their use should not be promoted within primary schools. Children are being encouraged (often by siblings) to look at or create their own sites and it is now widely regarded as an essential part of their social lives.

Advice in ***section 2.3.4*** of the ***Schools' e-Safety Policy Template*** booklet applies in all settings. Pupils should not upload photographs or videos of themselves or other pupils or staff without consent. They must not publish personal information, such as location and contact details and consideration should be given to advising pupils to use an anonymous nickname when logging into sites.

Identifying vulnerable groups

The use of handhelds, games consoles, Internet-enabled mobile phones and other technology both inside and outside of school is increasing rapidly. The most ICT capable may sometimes be the most vulnerable due to a lack of social and communication skills. Children who feel socially isolated may be more at risk from inappropriate online contact. Some children may not feel able to report a problem experienced online.

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. 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 and occasionally access 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. The incident should be logged and recorded by a member of the Senior Leadership Team. Parents should be notified if appropriate.*

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.

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/*** or ***www.bbc.co.uk/cbbc/find/***






Image searches are especially risky. There may be no need for pupils to download images if an adult downloads them before the lesson 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/*** or the NEN Gallery ***http://gallery.nen.gov.uk/***

For most curriculum-related research, there is no need to use an unfenced search engine; children could be directed to specific websites pre-selected by the class teacher. Safe and effective searching should be taught age appropriately as part of the ICT curriculum. At Key Stage One, this would be within a site e.g. BBC Schools or a Key Stage Two using a child-friendly search engine.

However, please note that **NO** filter-based search engine is completely safe.

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 a search within ***www.bbc.co.uk/schools***. Importantly, primary pupils can learn skills such as selecting keywords to narrow down searches, and to evaluate materials in terms of their quality and relevance. This will prepare them for efficient, productive Internet research in the secondary phase.

Webquests contain direct links to support pupil research thereby eliminating the need to use a search engine. Some webquests simply consist of a list of questions. The questions are linked directly to sources (i.e. suitable websites) and offer a motivating means of engaging reluctant readers in 'finding out'.

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. See: http://www.webquestuk.org.uk/

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.

Some useful resources and suitable websites for the Primary Classroom can be found below.

e-Safety in Communication:

www.kenttrustweb.org.uk/kentict/kentict_theme_esafety_comm.cfm

e-Safety in Research and e-Awareness:

www.kenttrustweb.org.uk/kentict/kentict_theme_esafety_research.cfm






Email

Most KCC primary schools use the email facility within Kent Learning Zone

https://portal.klz.org.uk

For external email, there is no need for pupils to use individual accounts. A 'class' email address should 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.kenttrustweb.org.uk/kentict/kentict_ict_easymail.cfm

Primary aged pupils should not be using web-based email systems that are not moderated by the school and not approved by KCC. This includes email systems such as Hotmail or Googlemail as these could allow children to exchange potentially inappropriate content without school knowledge.

Staff should not use home email accounts for school business. The Kent Learning Zone offers free email accounts to all staff in KCC primary schools. Staff using home email accounts for school business may place themselves in a difficult position as the data is not under their control and it is easier for social and school business messages to become mixed.

ICT subject leaders should keep their administrator account and password details in a safe place. Schools should ensure that more than one person has overall access to school email administrator accounts to avoid difficulties arising from staff being on leave, absent or no longer working with the school.

Teaching e-Safety

The Internet is an integral part of children's lives, whether we like it or not. There are ways for pupils to experience the benefits of communicating online with their peers, in relative safety.

The CEOP resources are a useful teaching tool for Key Stages One and Two looking at Internet safety and can be usefully incorporated into a PSHE or ICT programme. The Key Stage One area: Hector's world and the Key Stage Two area "Cybercafé" both have fully developed lesson plans and teaching materials available to download:

See ***www.thinkuknow.co.uk***

SuperClubs Plus is a subscription Social Networking site available on ***www.superclubsplus.com*** Superclubs Plus enables pupils 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.

Childnet International is a non-profit organisation working to "help make the Internet a great and safe place for children". Childnet have produced many materials to support the teaching of e-Safety at Key Stage One and Two. They have also produced materials for parents, staff and Secondary aged students. Their materials are available to access online or order from ***www.childnet.com***

For Kent materials and advice on teaching e-Safety, please see:
www.kenttrustweb.org.uk/kentict/kentict_esafety_home.cfm

Web Links

Signposts to Safety, Key Stage 1 + 2 version, Becta

http://publications.becta.org.uk






1.8 Routes to e-Safety — Secondary students

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

In writing their e-Safety Policies, secondary schools should consider these issues:

Guided educational use

Internet use produces significant educational benefits including access to information from around the world and the ability to communicate and publish widely. Internet use should be planned, task-orientated and educational. It should take place 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 education 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 reasonably protected. At an appropriate age and maturity 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. Students need to know how to cope if they come across inappropriate material or situations.

Students may access the Internet in Youth Clubs, Libraries, public access points and at home. 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 their local area.

Responsibility

e-Safety depends on schools, staff, governors, parents and the students themselves taking responsibility for their actions online. Staff have a particular responsibility to supervise students, plan access and be an appropriate role model. The balance between educating students to take a responsible approach and the use of regulation must be judged carefully.

Regulation

The use of the Internet 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, which are prominently displayed at the point of access, will help students make responsible decisions. Schools may wish to engage students in devising their own rules for responsible Internet use.

Students need to be taught what is acceptable and what is not, and to be given clear objectives for 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 are responsible for checking that filtering and monitoring is appropriate, effective and reasonable. Technical staff should not take the responsibility for educational or disciplinary issues.

Appropriate Internet access strategies

There are no straightforward or totally effective solutions and staff, parents and the students themselves must remain vigilant. The school should take all reasonable precautions to ensure that users access only appropriate material. Internet access and monitoring strategies will be selected by the school, in discussion with the filtering or Internet service provider where appropriate. The access strategy should be matched to the age, maturity 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 or network.

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.

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:

- Think U Know training which is provided by the CFE e-Safety Officer or other CEOP ambassadors.
- The Becta publication "Signposts to Safety: Teaching e-Safety at Key Stage 3 and 4" discusses in detail how e-Safety themes and ideas can be integrated with subjects across the curriculum.
- Reactive discussion when a suitable opportunity occurs.
- A range of appropriate materials are available via the Kent Trust Web site: See ***www.kenttrustweb.org.uk?esafety***

Schools should ensure that the use of resources by staff and 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 online and be shown how to validate information before accepting its accuracy. Students should be taught to acknowledge the author of the information used and to respect copyright when using material from the Internet 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.
- Know that illegal activities are strictly forbidden and may be reported to the authorities.
- Note that email is not guaranteed to be private.
- Know that system administrators monitor and have access to all email.
- Never share passwords with others.

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 students) are at the forefront of a huge range of new technologies and learning opportunities. This includes:

- Mobile phones may come with Internet, Bluetooth connectivity and a camera.
- New virtual learning environments such as Kent Learning Zone, Moodle and Becta approved learning platforms.
- The use of games and simulations to develop thinking skills.
- Internet voice and messaging systems such as Skype and VOIP (Voice over Internet Protocol).
- Digital storytelling and online publication such as Blogging, Wikis, Microsites.
- Podcasting, broadcasting and recording lessons.
- Digital video and video conferencing.

Web Links

Signposts to Safety, Teaching e-Safety at Key Stage 3 + 4 Becta

http://publications.becta.org.uk






1.9 e-Safety for vulnerable children and young people

In terms of e-safety information, ß'vulnerable' is a term of reference that would include children and young people who may:

- have special educational needs
- have been excluded
- demonstrate social / emotional / behavioural needs
- be Looked After Children
- be from ethnic minority groups
- be "at risk" in terms of safeguarding concerns

It is acknowledged that this group encompasses a large range of abilities and needs. There are common themes in their participation in e-safety initiatives:

Content	*Contact*	*Conduct*
Students who: Have inconsistent supervision and limited parent/carer awareness in home settings Don't understand the hidden/true meanings of inappropriate or advertising language Find it difficult to explain experiences verbally	**Students who:** Have limited understanding of online risk Have poor understanding of social uses of language for humour, sarcasm, compliments or street talk Are socially isolated children and young people Look for support in potentially inappropriate Internet forums	**Students who:** Find it difficult to stop and think about consequences of their actions Don't perceive that they have broken "netiquette" rules Don't understand how to respond to coercion Don't have adequate literacy skills to understand written rules and sanctions

It is typical practice to establish whole school e-Safety strategies to protect a cohort of children and young people. Strategies also need to provide the scope to include individual needs that vulnerable students may display. The impact of not considering individual requirements would be to increase the safety risks for these students. It is important to recognize that some students in this group will intentionally contravene rules and acceptable use policies. There would be an expectation that they would be subject to the same sanctions and consequences as peers if the evidence shows intent.

Potential incidents need careful investigation to consider a whole range of factors for children and young people in this vulnerable group. Investigation would be facilitated if the setting had profiled a student's needs and abilities clearly and shared these with any staff likely to use technology within curriculum delivery.

It is advisable to consult with the school SENCo for input into the writing of the e-Safety policy; this would provide a specialist perspective to synchronize support with policy.






There are four specific areas of concern that all schools should consider in their e-safety policy:

- Information presentation: can students read and understand words and messages?
- Communication skills: how will students communicate what has happened?
- Differentiation: do they remember concepts and ideas?
- Consistency: can they transfer skills from one activity to another?

There will need to be specific measures in place to ensure that all students and their parents/carers understand the meanings of "use" policies and the content of teaching activities and/or information posters or leaflets.

It is difficult to find generic resources for promoting and supporting e-safety for vulnerable groups as their needs are wide ranging. Resources that may help with communication skills are available from ***www.kentrustweb.org.uk/senict/*** e-safety for SEN.

Crick software have developed some resources in collaboration with Childnet International to provide Clicker 5 grids about their SMART rules ***www.learninggrids.com*** These are intended to support the existing resources from Childnet SMART adventures.

Please note that Guidance on the legal framework which could affect e-Safety issues and incidents can be found in section 5.0 of the e-Safety Policy Template.

For additional information and details about handling incidents in schools please refer to the '*Managing incidents in schools*' document:
www.kenttrustweb.org.uk/policy/managing_incidents.cfm

1.10 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 recognising concerns about pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to 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 Safeguards 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:** email and IM (Instant messaging)
- **Webcams and videoconferencing**
- **Online gaming**






What are the risks?

The risks that can be posed to young people and adults when online have been identified by the EUKids online project, which was later referenced in paragraph 1.3 of Dr Tanya Byron in "Safer Children in a Digital World" (2008).

	Commercial	*Aggressive*	*Sexual*	*Values*
Content (Child as recipient)	Adverts Spam Sponsorship Personal Info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (Child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (Child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading information/ advice

Byron Review (2008): ***http://www.dcsf.gov.uk/byronreview/***

How do we respond?

The Children's Safeguards Unit have worked with the County e-Safety Officer to provide guidance should you be concerned about Internet use by a child, young person or member of staff.

The flowchart on page 18 illustrates a suggested approach to managing an incident of concern. This diagram should not be used in isolation and the Children's Safeguards Unit can provide supporting documents to assist schools when responding to incidents.

General guidance following an incident

1) Record incidents in the e-Safety incident log and other relevant areas e.g. Bullying or Child protection log.
2) Ensure all appropriate staff are informed e.g. Senior Leadership Team, e-Safety Coordinator, Designated Child Protection Coordinator, ICT Coordinator/Manager, Chair of Governors etc.
3) After any investigations are completed it is essential to debrief, indentify lessons learnt and implement any changes required.
4) If at any time you are unsure how to proceed, then contact your Area Children's Officer for Child Protection or the County e-Safety Officer.

For additional guidance or contact information please see the Children's Safeguards Unit or e-Safety website:
www.kenttrustweb.org.uk?safeguards or ***www.kenttrustweb.org.uk?esafety***






Response to an Incident of Concern

e-Safety incident occurs

If a child is at immediate risk

Inform the Designated Child Protection Coordinator and follow schools' child protection procedures

Consult with Children's Safeguarding Unit (CSU)

Contact Kent Police (999) urgently if there is immediate danger

Contacts

Children Safeguard's Unit (CSU)
01622 696366
and speak to a local Children's Officer

e-Safety officer:
esafetyofficer@kent.gov.uk
01622 221469

Kent Police:
01622 690690 (Switch board)
ask to speak to the Public Protection Unit for your area and/or your Safer School Partnership Coordinator

Child Exploitation and Online Protection Centre (CEOP)
www.ceop.police.uk

Illegal Activity or Material found or suspected

- **Content**
  - Contact CSU or e-Safety Officer
  - Report to Internet Watch Foundation (www.iwf.org.uk) and/or Kent Police
- **Activity**
  - **Child**
    - Contact CSU and/or e-Safety Officer
    - Report to CEOP www.ceop.police.uk
    - Child protection procedures and/or criminal action
  - **Staff**
    - Contact CSU and/or e-Safety Officer
    - Report to CEOP www.ceop.police.uk
    - Staff allegations procedures and/or criminal action

Unsure

- Consult with CSU or e-Safety Officer

Inappropriate Activity or Material

- **Activity**
  - **Child**
    - **Possible School Actions:**
      - Sanctions
      - PSHE/citizenship
      - Restorative justice
      - Anti-bullying
      - Parental work
      - School support e.g. counselling, peer mentoring
      - Request support/advice from e-Safety officer
  - **Staff**
    - **Possible School Actions:**
      - Staff training
      - Disciplinary action
      - School support e.g. counselling
      - Request support/advice from e-Safety Officer
- **Content**
  - Report to filtering manager and/or Schools Broadband helpdesk

Review Schools e-Safety policies and procedures, record actions in e-Safety Incident log and implement any changes for the future






Responding to an Incident: Police procedures

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, schools should determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible, after contacting the Children Safeguard Team or e-Safety officer, if the offence is deemed to be out of the remit of the school to deal with.

Where it is determined that an offence has been committed and that a police investigation is warranted, all measures to preserve evidence should be undertaken.

If an Officer decides that equipment needs to be seized, then they will need to determine if the equipment is networked. If in doubt as to whether the server should be seized or not, officers should seek advice from the Police Digital Forensic Unit, as seizure of the server will have a significant impact on the school. It is **essential** that schools are aware of this possibility and they should ensure that measures are in place to enable the school's computer network to continue functioning should this situation arise.

In cases where a suspect picture or photograph is discovered it should also be borne in mind that a person could be guilty of the offence to 'Make' and 'Distribute' if they print or forward the image. There is a defence in law for these circumstances — in some cases, it may still be necessary for that person, or others (for example a person to whom an accidental find is reported), to knowingly "make" another copy of the photograph or pseudo-photograph in order that it will be reported to the authorities, and clearly it is desirable that they should be able to do so without fear of prosecution. Digital or printed copies of indecent images of children will be seized.

In all cases a detailed statement may be obtained to assist those who investigate the offence. The following information may be included in the statement:

- The identity of any material witnesses;
- The name of the Internet service provider (ISP) or mobile telephone service provider in the case of images received through a telephone;
- If known, the web address, name of the chat room or online group through which the image was found or received;
- Any passwords or other procedure required to gain access to the website;
- If known, the identity of the person who sent the image;
- In the case of email, the sender's email address or the screen name used by the sender while in a chat room;
- The reason for any delay in reporting the incident to the police (to assist investigators).

In the case of offences involving mobile telephones, the likelihood is that issues will in the main be resolved by the school. Should an incident arise which is deemed to be of a serious nature and necessitates criminal investigation it may require the seizure of the telephone.

The Safer Schools Partnership police officer responsible for the school should also be informed of any incident so that progress of any ongoing investigation can be monitored by them, and fed back to the school.






1.11 School responsibilities

e-Safety covers a wider scope than Internet use and a summary of a school's e-Safety responsibilities may be useful. This list should assist in developing a co-ordinated and effective approach to managing e-Safety issues.

The following should be considered:

- KCC 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 SLT, the ICT or PSHE subject leader or a subject teacher. The e-Safety Coordinator should not be a member of the technical staff.
- The e-Safety Coordinator can request and access support and advice from the CFE e-Safety Officer, the Children's Safeguard Service and where necessary, the Police. e-Safety training is also available through the Advisory Service CPD Programme and the KSCB. A full list of recommended responsibilities for the e-Safety Coordinator can be found in Becta's "AUP's in Context: Establishing Safe and Responsible Online Behaviours" ***http://publications.becta.org.uk/display.cfm?resID=39286***
- 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 logged and investigated where appropriate by Senior Leadership Team, the Children's Safeguard Service or the Police.
- Schools should consider e-Safety whenever they are using the Internet and ensure that every pupil has been educated about safe and responsible use e.g. as part of the PSHE curriculum. Pupils and staff need to know how to minimise online risks and how to report a problem.
- Schools should refer to e-Safety policies and procedures within their Self-evaluation Form (SEF). Schools can use the e-Safety Audit Tool to support this.
- All staff should agree and sign the School's Code of Practice for ICT.
- Parents should sign and return the Acceptable Use Policy and comment 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 suggestions may be useful:

- e-Safety awareness is an essential element of all staff and volunteer induction.
- The audit tool provided in the Core e-Safety Policies is a good place to start when checking the school's e-Safety readiness
- Pupils should be reminded of their responsibilities whenever they are using the Internet. Displaying and referring to posters in rooms with Internet access is one useful approach.
- Ensure all staff, pupils and parents know how to report an incident of concern regarding Internet use.
- Make sure a member of the senior leadership team (if filtering is managed locally) approves the school filtering configuration and supervise the staff who manage the filtering system.

For further information and an e-Safety audit please visit the e-Safety site:
www.kenttrustweb.org.uk?esafety






1.12 Use of Social Media Tools as a school or establishment

Social Media tools, such as blogs, Wikis, social networking sites and video sharing sites (such as Twitter, YouTube, Facebook etc.) can be fantastic for teaching and learning. These tools can also help to engage with parents/carers and the wider community. However it is essential that their use is carefully considered by a school.

Good e-Safety practice must be fully embedded across the establishment (such as whole staff e-Safety training, Social Media 'training' for staff and students and parental awareness inputs) before schools can consider using Social Media tools.

The decision on using Social Media tools must be made as a school and should only take place with full support and backing by the Senior Leadership Team. The use of Social Media tools must be fully documented and risk assessed and outlined in the e-Safety Policy (section 2.3.5 in the Policy Template). The school will need to be aware of their responsibility to moderating any content and to ensure that the service is kept up to date. The tools must also be used in accordance with the school's behaviour and complaints policies.

Firstly, it is essential that the correct tool is selected, for example to communicate with parents and carers about school based decisions it might be better to use a blog to enable a discussion rather than a Twitter page. Schools should also – where possible – use tools available on their school website or Learning Platform. Kent Learning Zone for example can offer the use of Blogs, Wikis etc for pupils, staff and parent/carers in a closed but controlled environment.

Crucial to selecting the appropriate Social Media tool is deciding who the target audience is (parents/carers or pupils etc). Schools will need to be aware that not all families will have access to technology at home. To combat this issue some schools have offered open evenings to families or have an internet enabled computer in an accessible location for parents/carers to access after signing an Acceptable Use Policy. It is also important to find out if your audience would like to engage with the school via such media, for example some students may not wish to add their school on a social networking site!

It is important that schools are aware how Social Media sites function and are aware how to make them as safe as possible, such as making profiles "private" or using groups to engage with the community instead of profiles.

When using Social Media with children, schools must be aware of site age restrictions and only use sites that are deemed to be age appropriate and suitable for educational purposes. Such tools will also need to be moderated and regulated frequently as very few social media tools are able to verify and authenticate users appropriately, unless the system is controlled directly by the school or by a subscription service such as Kent Learning Zone, Ning, ELGG, Super Clubs, RadioWaves etc. Where possible when using services which the school cannot control (e.g. Facebook, Twitter, YouTube) then it is recommended that comments etc are approved before they are made live and membership to online groups etc is controlled (e.g. people must request to join a group or follow).

In order to protect staff, professional accounts, pages or profiles must be used when communicating with pupils or the school community. School approved email addresses and contact details should be used and staff should not share any personal contact details or information with pupils or parents/carers.

Schools can also consult with the e-Safety Officer to discuss ideas and options before using social media tools with students or the community ***esafetyofficer@kent.gov.uk***






The KSCB document "*Safer Use of New Technology*" discusses more ideas on how to use technology when working with young people and can be found at ***www.kenttrustweb.org.uk?esafety***

Childnet have also considered using Social Networking sites to engage with young people and the community and have some useful tools and ideas at ***www.digizen.org.uk/socialnetworking***

The "*Guidance for Safer Working Practice for Adults who Work with Children and Young People*" document updated in January 2009 and produced by the DCFS, also has recommendations for adults using technology to communicate with children and young people ***http://www.dcsf.gov.uk/everychildmatters/_download/?id=5824***






Acknowledgements

This edition has been the work of:

Rebecca Avery, CFE; Peter Banbury, ISG Commissioning; Heidi Barton, ASK; Alan Day, CFE; Rachel Keen, SENICT; Steve Moores, Maidstone Grammar; Mike O'Connell, CFE Child Protection; Godfrey Pain, Kent Police; Marc Turner, EIS; Carol Webb, Invicta Grammar and Pam Wemban, Riverview Junior School.

The seven 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; Mandy Barrow, ASK; Clive Bonner, EIS; Martin Carter, SEGfL; 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, Kent; 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, ISG; Chris Ridgeway, Invicta Grammar; Nick Roberts, Sussex LEA; Graham Stabbs, St Margarets at Cliffe Primary; Sharon Sperling, Libraries; Brian Tayler, ISG; Joanna Wainwright, KCC; Richard Ward, KCC; Theresa Warford, Libraries; Ian Whyte, Plaxtol Primary; Chris Woodley, KCC; Rebecca Wright, CFE; Heather Pettitt, SEGfL; Ian White, SWGfL; Greg Hill, SEGfL.

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