E-Safety Policy

As a school we are committed to ensuring the best safeguarding procedures are in place and see e-safety as a high priority in ensuring the safety and welfare of our children.

This policy should be read in conjunction with other policies including those for **behaviour, safeguarding and anti-bullying**

Using this policy

All staff are responsible for promoting and supporting safe behaviours and for following e-safety procedures. They are aware of their own personal responsibilities to protect the security and confidentiality of the school network.

- The Senior Leadership Team will discuss current ICT issues termly and also share with staff at briefings.
- Any e-safety concerns in the school should be reported to the Headteacher or Deputy in accordance with our safeguarding policy.
- Our e-safety policy has been written, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The e-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the site. This includes but is not limited to workstations, laptops, mobile phones and tablets used on the school site.
- The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help children to learn how to assess and manage risk. Children will be taught to keep themselves safe when using the internet and taught how to bridge the gap between school IT systems to the more open systems used outside of these settings.

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Surrey County Council can accept liability for the material accessed, or any consequences of internet access.

- The school will use a recognised internet service provider or regional broadband consortium and this is reviewed regularly.
- The school has a contract with an internet provider to ensure that all internet access has age appropriate filtering system.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school network is controlled by personal passwords. Children accessing the system have individual log-ins using their own username.
- All staff follow clear procedures for reporting issues and a log of any incidents will be passed the e-safety co-ordinator and/or DCPO. These are kept to help to identify patterns of behaviour and to inform the e-safety policy.
- The school will ensure that one-off visitors, members of the community and other organisations who visit are made aware of the school policy when they sign-in.
- Regular contractors, members of the community and other organisations who let the building and access the internet via their own personal devices will sign a Partnership Agreement so it is expected that their use will be in accordance with the school e-safety policy.

Internet Use

The school will provide an age-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

All communication between staff, pupils and families will take place using school equipment or accounts. Any contact details given, such as address, email and telephone number, will be of the school. Staff or pupils' personal information will not be published.

In accordance with the Acceptable Use Agreements which are signed annually, staff and pupils should ensure that their online activity, both in school and out is appropriate for their situation as a member of the school community.

In school, teachers have the responsibility to teach e-safety lessons at least every half term. The school will provide an age-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Teachers will also use these sessions to concentrate on any issues arising in their class.
Pupils are taught not to give out personal details or information which may identify them or their location. They will be reminded about the 'Responsible Use' policy which they have agreed to.

E-mail

- Pupils and staff may only use approved e-mail accounts to communicate with parents/carers and other professionals.
- Staff to pupil email communication must only take place via a school email address.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. http://www.surreycc.gov.uk/?a=168635
- School would usually only print first names of pupils

Social Media

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- There is a separate social media policy covering the school's own accounts
- Staff and pupils should use ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.
-

Use of personal devices

- Personal equipment may be used by staff and/or pupils to access the school IT systems provided their use complies with the e-safety policy and the relevant Acceptable Use Agreement.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data

- The school has a separate Data Handling Policy. It covers the use of external data storage, access to pupil and staff personal data on and off site, remote access to school systems.

Policy Decisions

Authorising access

- **All** staff, governors, students and volunteers must read and sign the 'Staff Acceptable Use Policy' annually.
- At Key Stage 1, access to the internet will be supervised by an adult with guidance on how to access to specific, approved on-line materials.
- Supply teachers and students will be given separate log-on information for the computers so that sensitive information cannot be accidentally accessed by them.
- At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy, as appropriate to the needs and abilities of the children.
- All parents and pupils will be asked to sign and return a consent form agreeing to 'Responsible Use'
- Parents' and carers' attention will be drawn to the School and Children's Centre e-safety Policy in newsletters, the school brochure and on the school web site.
- **Assessing risks**
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints

- Complaints of internet misuse should be reported to the Headteacher and will be dealt according to the relevant policies.
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behaviour policy.

Community use of the internet

- Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school e-safety policy.

Communication of the Policy

To pupils

- Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet
- Pupils will be reminded about the contents of the AUP as part of their e-safety education

To staff

- All staff will be shown where to access the e-safety policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet
- All staff will receive e-safety training on an annual basis

To parents

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school web site.
- Parents will be offered e-safety updates annually and full training every two years

Policy review:

Date discussed by staff: Autumn Term 2015

Date reviewed by governing body: Autumn Term 2015

Date due for review: Autumn Term 2016

Appendices

Appendix 1	Staff and Governor acceptable user agreement
Appendix 2	Visitor acceptable user agreement
Appendix 3	E-safety rules for KS1 and KS2
Appendix 4	Parent ICT user agreement on behalf of their child
Appendix 5	Responding to an e-safety incident
Appendix 6	E-Safety Incident Log
Appendix 7	Proposed responses to e-safety incidents by children matrix
Appendix 8	The Legal Framework surrounding e-safety

Appendix 1 – Staff and Governor acceptable user agreement

Staff, Governor, Volunteer and Student Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the School's e-Safety coordinator.

- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email, internet and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will only use the approved, secure email system(s) for any school business. If any in appropriate content is detected the email account must be closed immediately. If liaising with parents via email I understand that the school email account needs to be used.
- I will ensure that all electronic communications with parents, pupils and staff, including email, IM and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school on an encrypted USB disk or accessed remotely when authorised by the Head teacher or Governing Body.
- I agree not to use 'cloud based storage systems' to store any personal or sensitive data on.
- I will only take images of pupils and/or staff for professional purposes in line with school policy. I will not distribute images outside the school network/learning platform without the permission of the Head teacher.
- I will not install any hardware or software without the permission of the school.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- Following **Guidance on the Use of Email and Text Messaging by Professionals and E- Safety Safe Practice with Technology** I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support the school's e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the e-safety Coordinator, the Designated Child Protection Officer or Head teacher.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serous infringements may be referred to the police.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school/ Children's Centre.

Full Name…… (Printed)

Job title……

Signature…… Date……

Appendix 2 – Visitor acceptable user agreement

Visitor
Acceptable Use Agreement / Code of Conduct

- I understand that I have been given use of the school internet and/or school ICT systems in order to carry out a specific job for the school
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email, internet and any related technologies for the purpose for which I have been given access.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will not install any hardware or software without the permission of the school.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory whilst using the school ICT systems
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Head teacher or my employer.
- I will respect copyright and intellectual property rights.
- I understand that if I disregard any of the above then it will be reported to my employer and serious infringements may be referred to the police.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name…… (Printed)

Company……

Signature…… Date……

Appendix 3 - E-safety rules

Key Stage 1

Think then Click

These rules help me to stay safe on the internet

I will take care of the school computers

I will only use the internet when I have been given permission by an adult

I will tell an adult if I see something on the internet that upsets me.

I will not tell other people my personal things about me.

I will always be polite and friendly when I write messages on the internet

Always remember

Treat your password like your toothbrush; don't let anyone else use it!!

Always let an adult know if something on the internet worries you.

Key Stage 2

Acceptable use of the school computers

These rules will help to keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework
- I will not tell anyone my login and password
- I will only login to the school systems as myself unless I have been given permission to do otherwise
- I will only edit or delete my own files
- I am aware that some websites and social networks have age restrictions which mean that I should not go on them
- I will only visit internet sites that are appropriate for my age and immediately close down any webpage I don't like
- I will only communicate with people I know, or that a responsible adult has approved and will never arrange to meet with someone I don't know
- I will only send polite and friendly messages
- I will not open an attachment, or download a file, unless I have been given permission by an adult
- I will not tell anyone my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- If I see anything I am unhappy with or I receive a message I do not like, I will show a responsible adult.

I agree to follow these internet safety rules

My name: . . . . . Class: . . . . . Date: . . . . . .

Always remember

Treat your password like your toothbrush; don't let anyone else use it!!

Always let an adult know if something on the internet worries you.

Appendix 4 – Parent ICT user agreement on behalf of their child

Dear Parents/Guardians,

Use of the Internet in school is a vital part of the education of your son/daughter. As required by the National Curriculum all pupils use computer facilities, including internet access, as an essential part of learning,. Both pupils and their parents/carers are asked to sign agreements to show that the e-safety Rules have been understood and agreed.

I know that my daughter or son has signed an e-safety agreement form and that they have a copy of the school e-safety rules. We have discussed this document and my daughter or son agrees to follow the e-safety rules and to support the safe and responsible use of ICT at St Lawrence C of E Primary School.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files and the internet sites that they visit, and that if they have concerns about their e-safety or e-behaviour they will contact me.

I understand the school is not liable for any damages arising from my child's use of the internet facilities.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Pupil name: …… Class: .....

As the parent or legal guardian of the above pupil, I have read and understood the attached school e-safety rules and grant permission for my daughter or son to have access to use the internet, school email system and other ICT facilities at school.

Parent / Carer name: ……

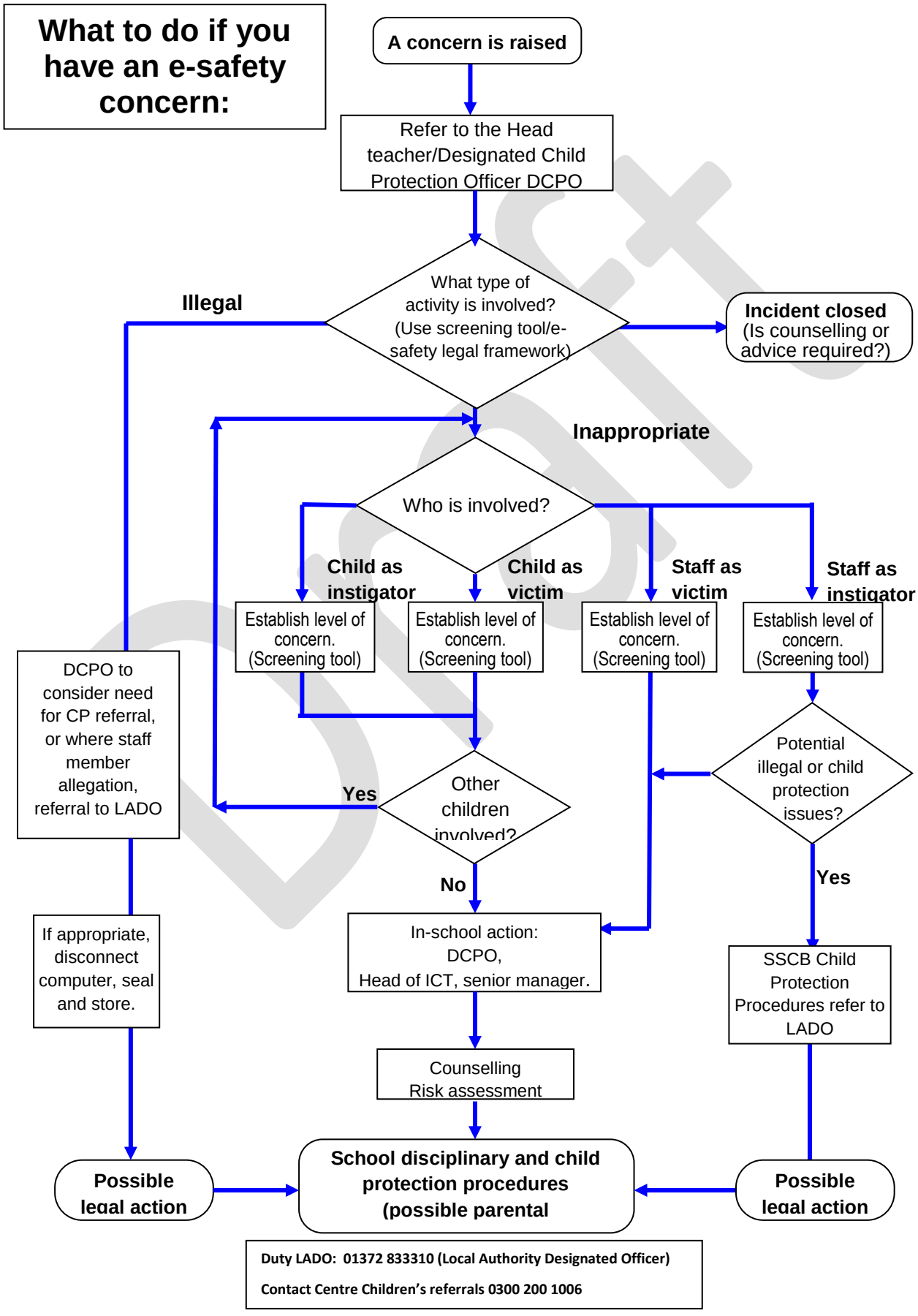
Parent/Guardian signature: …….. Date.....

Please complete, sign and return one copy to your child's class teacher

Appendix 5 - Responding to an e-safety incident

This guidance is for senior management within schools on how to respond to an e-safety incident of concern. It is important to note that incidents may involve an adult or child as the victim or the instigator. Adults are also subject to cyber bullying by pupils.

This diagram should be used with the screening tool and the Surrey Child Protection Procedures which include what to do if you are concerned about a child, or about an adult working with children. Schools' DCPOs will be conversant with these and the processes for referral.



E-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	

Appendix 7- Proposed responses to e-safety incidents by children matrix

The following matrix offers examples of typical incidents and suggestions as to possible responses.

Child as victim

Child as victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Receiving unsolicited content that is inappropriate, obscene, offensive or threatening	Web sites (often through mis-clicked or mis-typed web addresses); email (Spam); banner advertising; pop-ups (largely eradicated through better browser design).	Educator vigilance; Acceptable internet Use Policy known by all users, and is enforced by school. Effective web filtering in place. Using safe filtered email. Effective spam filtering. Maintain email and URL logs and history.	Complete a risk assessment to determine severity of impact on the child. As the content is unsolicited, there can be no question of culpability of the child. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate. Ensure incidents are reported and recorded.	*All secondary children should have access to the internet and personal email as an entitlement. Protective measures are essential; however it is not acceptable to be so risk averse that access is removed entirely. There should be procedures agreed with parents and Governors for reporting abuse.*

Child as victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Child is the subject of published material.	Images stored in publicly accessible areas; Personal blogs such as MSN spaces, BEBO etc.; Details left on web sites. Incitement: hatred and discrimination, personal harm etc.	Educator vigilance; Acceptable internet Use Policy known by all users, and children made aware of the dangers.	Complete a risk assessment to determine the severity of impact on the child. Determine if a perpetrator / victim relationship may exist. Where an in-school perpetrator is identified, and a crime has taken place, police should be informed. Disciplinary action may follow. Where an external perpetrator is identified, report to police. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate.	*Most image storage sites have levels of access, usually private; family & friends and public. These sites are great fun for sharing images; however care should be taken, as users may be able to access inappropriate images posted by others.*

Child as victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Bullying and threats.	Email; text messaging; blogs; sexting; self-harm sites, drug forums; suicide sites; hate sites; Instant Messenger. Incitement: hatred and discrimination, personal harm etc.	Reinforcement of school ethos and behaviour. Regular sample trawls of known sites. Anti-bullying initiatives should accompany efforts to promote internet use	Complete a risk assessment to determine the severity of impact on the child. Determine if a perpetrator / victim relationship exists. Where a perpetrator is identified take appropriate disciplinary action. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate. Online and offline bullying should be seen as connected. Although children have a range of coping mechanisms, support is needed for the victim to ensure as often they do not tell a trusted adult or friend. The bully themselves may be vulnerable so appropriate counselling will also be needed. Raising awareness for teachers, parents and students about the array of risks that keep changing on the internet.	*There is no real difference between bullying and threats using technology and more familiar means. Bullying and threatening behaviour is damaging and wrong and should be treated very seriously.*
Security	Adware; browser hijack; virus.	Secure and up to date browser settings and anti-virus software; regular adware scans.	Effective reactive technical intervention.	*This is a frequent problem that is amplified where operating systems and browsers are not regularly updated. It can often occur where inappropriate sites have been visited.*
Predation and grooming	Forming online relationships by deception with the intent of gaining the confidence of a minor to do harm.	Teach awareness of dangers. Use the 'Think U Know' teaching resources.	Where a perpetrator is identified, take appropriate disciplinary/legal action and in the first instance refer to police. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Early advice to parents with regard to computer and games console locations, use and mobile technology.	*Grooming and predation is a child protection issue and should be reported to social care/ police in all cases, or referred to the CEOP through their reporting web site.*

Child as instigator				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Soliciting content that is inappropriate, obscene, or offensive.	Use of inappropriate search terms; Accessing or forwarding the details of known sites; Following inappropriate links or banners; inappropriate Image searches.	Use safe image search engines. Effective web filtering. Educator vigilance. Effective incident reporting procedures for blocking sites once known.	Inform parents (consider standard letter templates). Restrict computer or internet access for a fixed period, dependent on severity. Maintain incident records to identity patterns of behaviour. -If a crime has taken place, report it to the police i.e. making /distributing images or communications offences	*Maintain records of incidents to identify serial offenders.*
Sends or publishes content that is inappropriate, obscene, offensive or threatening.	Emails blogs; msn-spaces; social sites (BEBO etc.) chat rooms.	Block access to specific sites.	Maintain records of incidents to identify regular offenders. Inform parents. (Consider standard letters). Remove computer access for a fixed period. -If a crime has taken place, report it to the police i.e. making /distributing images or communications offences	*The medium is less important than intent. Publishing is easy using the web; however in legal terms it can still be libellous and subject to the same legal remedies. Where there are known sites that do not moderate effectively they should be blocked.*
Identity Theft, personal information abuse,	Using others identity to gain access to school systems or services.	Systematic changes of password. Alternative methods of authentication, such as swipe card or fingerprint.	Recover identity and change password. Inform parents (standard letter templates). Restrict computer or internet access for a fixed period, dependent on severity. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required.	*It is essential that schools consider carefully where personal data is stored, and who can access this data. Access to names and addresses must be secure, and CRB checks in place to protect children.*
Requests for personal information, financial cheating	'Phishing' is the use of deceit to obtain personal (usually financial) information.	Teach awareness of dangers.	If identity theft occurs it should be reported to police without exception.	*Most 'phishing' is aimed at adults with banking facilities, so older children are more likely to be affected.*

Appendix 8 - The Legal Framework surrounding e-safety

This section is designed to inform users of legal issues relevant to the use of electronic communications. It might also be useful to make reference to this when dealing with e-safety infringements to reinforce the seriousness of issues arising.

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 committed as soon as the message has been sent: there is no need to prove any intent or purpose.

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 (DOS) attacks).

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

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.

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.

Education Act 2011, sections 2 to 4,

This provides further clarification on statutory staff powers to discipline pupils for inappropriate behaviour or not for following instructions, both on and off school premises. Further details for Free schools can be found in section 36 and for Academies in Part 6, sections 55 to 65.

Education and Inspections Act 2006, sections 90 and 91

This provide statutory powers for staff to discipline pupils for inappropriate behaviour or for not following instructions, both on and off school premises. **Section 94** also gives schools the power to confiscate items from pupils as a disciplinary penalty. These powers may be particularly important when dealing with e-safety issues: online bullying may take place both inside and outside school, and this legislation gives schools the legal power to intervene should incidents occur. It also gives teachers the power to confiscate mobile phones, and other personal devices, if they suspect that they are being used to compromise the well-being and safety of others.

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.

Obscene Publications Act 1959 and 1964

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

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.

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.

The Equality Act 2010

The Equality Act 2010 provides a single, consolidated source of discrimination law, covering all the types of discrimination that are unlawful. It defines that schools cannot unlawfully discriminate against pupils because of their sex, race, disability, religion or belief and sexual orientation. Protection is now extended to pupils who are pregnant or undergoing gender reassignment. However, schools that are already complying with the law should not find major differences in what they need to do.

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 abuse based on their race, nationality or ethnic background.

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.

Sexual Offences Act 2003

A 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) and then intentionally meet them or travel with intent 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 should already have a copy of "Children & Families: Safer from Sexual Crime" document, which is available from the Home Office website (www.homeoffice.gov.uk/documents/children-safer-fr-sex-crime?view=Binary).

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