

# Policy for Online Safety



## 1. RATIONALE

We believe that access to the Internet offers a rich environment for both pupils and staff and that the Internet is an essential element in 21st century life for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. We believe that the potential benefits to pupils from access to information resources far exceed the disadvantages. As part of the children's learning across subjects we will be offering pupils supervised access to the Internet. Before being allowed to use the Internet all pupils must have parental permission to do so.

At Crawley Ridge, we believe that the potential benefits to pupils include the following:

- Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use
- Pupils are educated in safe searching when using the Internet, and will be directed to safe and age appropriate digital resources
- Pupils are taught about how to stay safe on the Internet and how to behave appropriately and responsibly
- Pupils are shown how to publish and present information appropriately to a wider audience
- Pupils are prepared to use online communication tools effectively and safely.

Our Online Safety policy has been written by the school, building on best practice and government guidance.

## 2. PROCEDURES / GUIDANCE FOR USE

### 2.1 Managing access and security

- The school is using a recognised internet service provider or regional broadband consortium
- The school will ensure that all internet access has age appropriate recognised filtering which is regularly checked to ensure that it is working, effective and reasonable
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator (Miss Humphrey)
- The School Bursar will ensure that its networks have virus and anti-spam protection and a weekly report is generated

- Access to school networks will be controlled by personal passwords except for children, who have limited access
- School IT systems security is reviewed regularly.

## **2.2 Internet Use**

- The school will provide an age-appropriate online 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 and pupils or families will take place using school equipment and school accounts
- Pupils will be advised not to give out personal details or information which may identify them or their location
- Pupils will be issued with passwords for Purplemash and are advised of the implications that may occur if someone finds this out and accesses their account

## **2.3 Email**

- Pupils and staff may only use approved email accounts on the school IT systems
- Children may use class-based email accounts, when appropriate, to send internal messages only.
- Staff to pupil and pupil to staff online communication must only take place via a school email address
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.

## **2.4 Published content eg the school website**

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published
- The Headteacher will take overall editorial responsibility and ensure that the content is accurate and appropriate.

## **2.5 Publishing pupils' images and work**

- Parents are clearly informed and reminded of the school policy on image taking and publishing onto social media or other online platforms (especially during school performances)
- Please see school photographic policy for further information.

## **2.6 Videoconferencing**

- Videoconferencing/ Skype will use the educational broadband network to ensure quality of service and security rather than the Internet
- Videoconferencing/Skype will only take place through appropriate teacher supervision.

## **2.7 Emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Staff will use a school phone where contact with pupils or parents is required.

## **2.8 Use of personal equipment**

- Mobile phones with cameras will not be used during lessons or formal school time but may be used for communication on outings for necessary contact between the staff and the school office
- Personal equipment may be used by staff to access the school's IT system provided the use complies with the Online Safety policy and the relevant Acceptable Use Policy
- Staff must not store images of pupils or pupils' 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.

## **2.9 Protecting personal data**

- The school has a separate Data Protection Policy

## **2.10 Authorising Internet access**

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, IT technicians and governors) must read and sign the 'Acceptable Use of IT for staff and governors before using any school IT resource. See Appendix 1
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems
- Teaching staff demonstrate effective use of the Internet. Access to the Internet is supervised by adults and children are guided to use appropriate sites
- Parents are asked to sign and return an Internet consent form on entry to the school. See Appendix 3
- Any person not directly employed by the school will be asked to sign Acceptable Use of IT Agreement for visitors and volunteers (see appendix 2) before being allowed to access the Internet from the school site.

## **2.11 Assessing risks**

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the nature of the Internet, 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.

## **2.12 Handling Online Safety complaints**

- 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
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

## **2.13 Community use of the Internet**

- All use of the school Internet connection by community and other organisations shall be in accordance with the school Online Safety policy and potential IT users will be expected to sign the AUP.

## **2.14 Introducing Online Safety to pupils**

- The school Online Safety programme teaches children about relevant safety issues and instil a set of safe behaviours when accessing the Internet. Online safety lessons are planned and taught regularly throughout the school as part of the Computing curriculum and the Keeping Safe module of the PSHE curriculum
- Online Safety rules are posted in all school learning areas where computer access for the children is most frequently available ( Appendix 4)
- Pupils are informed that network and Internet use will be monitored
- Pupils will be taught how to evaluate Internet content
- The school will seek to ensure that the use of Internet derived material by staff and by pupils complies with copyright law.
- Where possible, pupils are encouraged to verify the information they find online with other sources, e.g. books
- Pupils are advised never to give out personal details of any kind which may identify them or their location, including uploading photos of themselves in their school uniform
- Pupils are advised to use nicknames and avatars when using social networking sites and to send kind messages to others as well as to report anything suspicious that they do not like by telling an adult straight away
- Pupils are taught how to report content that concerns them to a member of teaching staff. The school uses the Windows D function to hide content the children may find concerning and they are then able to seek an adult to support them.

## **2.15 Staff and the Online Safety policy**

- All staff will be given the School Online Safety Policy and its importance explained
- Staff will receive regular online safety training
- All staff must sign and agree to comply with the Staff Acceptable Use Policy in order to gain access to the school IT systems and the internet on site
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

## **2.16 Parental support**

- This policy may also be found on the school website.
- The school informs parents about online safety through updates via parentmail and through the Online Safety Guidance page on the school website
- The school will maintain a list of recommended online safety resources for parents/carers to use in reinforcing messages of online safety outside of school.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

## **3. MONITORING EVALUATION AND REVIEW**

Our Online Safety Policy has been written by the school, building on best practice and government guidance. The school audits IT use and emergence of new technologies to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

The policy will be reviewed on a two year cycle by the Online Safety leader, the Healthy Schools Lead, teaching staff and the Governors' Children and Learning Committee.

#### **4. LINKS TO OTHER POLICIES/ USEFUL WEBSITES**

- Computing Policy
- Anti-bullying
- PSHE
- Safeguarding and Child Protection
- E-Safety Toolkit for Schools SCC June 2014
- [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
- [www.kidsmart.org.uk](http://www.kidsmart.org.uk)
- [Www.yhgfl.net/eSafety/Parents](http://Www.yhgfl.net/eSafety/Parents)

**Date of completion: January 2018**

**Date of adoption: March 2018**

**Date for review: Spring 2019**

## Appendix 1



### **Staff, Governor and Visitor Acceptable Use of IT Agreement updated January 18**

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 to its contents at all times. Any concerns or clarification should be discussed with Miss Humphrey who is the Online Safety coordinator.

- I appreciate that IT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business.
- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the IT 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.
- I will ensure that all electronic communications with parents, pupils and staff, including email, Instant Messaging 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 or accessed remotely when authorised by the Head teacher or Governing Body.
- 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 Headteacher or Bursar
- 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.
- 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 Online Safety policy and help pupils to be safe and responsible in their use of IT and related technologies. I will promote Online Safety with children 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 Online 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 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)

Job title.....

Signature..... Date.....





## Appendix 2



### Visitor /Volunteer Acceptable Use of IT Agreement

I understand that I have been given use of the school internet and/or school IT systems in order to carry out a specific job for the school

I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.

I will only use the school's email / internet / intranet / Learning Platform and any related technologies for the purpose for which I have been given access.

I will comply with the IT 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 Headteacher or Bursar

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory whilst using the school IT 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 IT throughout the school.

Full Name..... (Printed)

Company.....

Signature..... Date.....

**APPENDIX 3  
ACCESS TO THE INTERNET**

All pupils use computer facilities, including internet access, as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign agreements to show that the Online Safety Rules have been understood and agreed.

**Parent / Carer name:** .....

Pupil name: .....

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

I know that my daughter or son will be taught about online safety rules as an integral part of the Computing and PSHE curriculum and Online Safety rules are displayed throughout the school in computer use areas. We have discussed this document and my daughter or son agrees to follow the online safety rules and to support the safe and responsible use of ICT at Crawley Ridge Infant 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 online 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 online safety or behaviour online they will contact me.

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





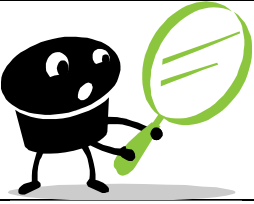


I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/Guardian signature:

.....Date.....

**Please complete, sign and return to**

Appendix 4

	<p><b>Golden Rules</b></p> <p><b>Think then Click</b></p> 
	<p><b>We only use the internet when an adult gives us permission</b></p>
	<p><b>We can click on buttons and links when we know what they do</b></p>
	<p><b>We can search the internet with an adult</b></p>
	<p><b>We always ask if we get lost on the internet</b></p>
	<p><b>We can write polite and friendly Messages</b></p>
	<p><b>We will not share our purple mash passwords</b></p>
	<p><b>If you don't like what you see, press Windows D</b></p>

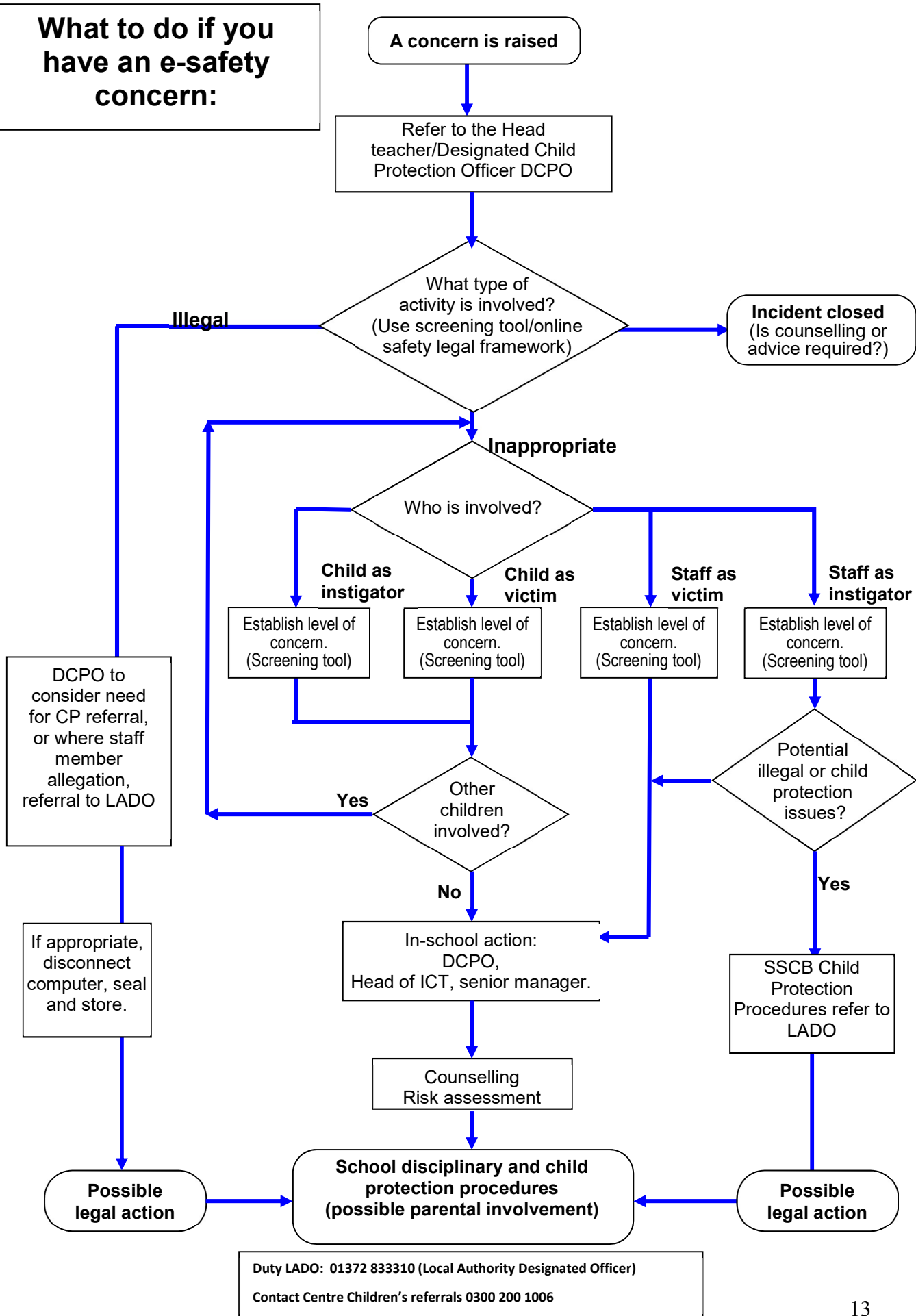
## **Appendix 5**

### **Responding to an Online Safety incident**

This guidance is for senior management within schools on how to respond to an online 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.

The first section outlines key online safety risk behaviours. The flowchart on page 4 illustrates the approach to investigating an incident of concern. 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.

# What to do if you have an e-safety concern:



## Appendix 6

### Proposed responses to online 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.	<i>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.</i>

<b>Child as victim</b>				
<b>Hazard</b>	<b>Examples</b>	<b>Prevention</b>	<b>Proposed Response</b>	<b>Comments</b>
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.	<i>Most image storage sites have levels of access, usually private; family &amp; 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.</i>

<b>Child as victim</b>				
<b>Hazard</b>	<b>Examples</b>	<b>Prevention</b>	<b>Proposed Response</b>	<b>Comments</b>
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 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.	<i>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.</i>
Security	Adware; browser hijack; virus.	Secure and up to date browser settings and anti-virus software;	Effective reactive technical intervention.	<i>This is a frequent problem that is amplified where operating systems and browsers are not regularly updated. It can often</i>



		regular adware scans.		<i>occur where inappropriate sites have been visited.</i>
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.	<i>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.</i>
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.	<i>Most 'phishing' is aimed at adults with banking facilities, so older children are more likely to be affected.</i>

<b>Child as instigator</b>				
<b>Hazard</b>	<b>Examples</b>	<b>Prevention</b>	<b>Proposed Response</b>	<b>Comments</b>
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 identify patterns of behaviour. -If a crime has taken place, report it to the police i.e. making /distributing images or communications offences	<i>Maintain records of incidents to identify serial offenders.</i>
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	<i>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.</i>
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	<i>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,</i>

Child as instigator				
			recurrence, including ensuring that relevant sites are blocked if required.	<i>and CRB checks in place to protect children.</i>