ONLINE SAFETY POLICY

Introduction

Significant educational benefits result from curriculum Internet use, including access to information from around the world and the ability to communicate widely. Internet safety depends on staff, schools, governors, advisers and parents taking responsibility for the use of the Internet.

The Internet is an essential element in life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement and to support the professional work of staff. One benefit of using the Internet is that it allows access to world-wide educational resources including museums and art galleries. Staff have a professional responsibility to ensure that users are taught to access appropriate material.

Curriculum Intent

We want to ensure that our children are able to use the Internet and related communications technologies appropriately and safely. Effective use of the Internet is an essential life-skill. Unmediated Internet access brings with it the possibility of placing of pupils in inappropriate and even dangerous situations. We aim to create a safe IT learning environment to ensure that everyone is aware of the issues and how they impact upon the particular school environment and the pupils within the school. We need a policy to help to ensure responsible use and the safety of pupils.

Who is covered by the policy?

This policy relates to all children and adults who use any IT equipment in school – this may include PCs, laptops, ipads, notebooks, tablets, smart phones, memory sticks or any other new technology with similar applications. It also relates to children and adults working off-site, for example at home, but accessing the school website, learning platform or other applications recommended by school as part of school work.

Legal Issues

All of the school's software is legally licensed and catalogued. No software can be added to machines unless permission has been given by the school's Computing Leader. No material is to be shared (either via e-mail or via the school's website) until it has been checked. This will ensure that no copyright laws are broken.

Implementation of the policy

Inappropriate material

Unfortunately, along with a wealth of useful educational sites on the Internet, there are also sites which contain inappropriate materials which it would be unacceptable for children to gain access to.

To ensure that children access the Internet within a safe environment, we use LEAD IT Services as our Internet Service Provider (ISP). The ISP ensures that filtering unacceptable material through filtering lists of inappropriate sites to which access is barred when using the school's line. However, there is a very small risk that inappropriate material may occasionally get through unfiltered.
We therefore follow the agreed guidelines below to ensure that children can access the Internet safely.

Guidance for staff

Teachers should:

- Ensure that they have received adequate training with Internet use before they supervise children's use of the Internet.
- Supervise children *at all times* when accessing the Internet, with all monitors clearly visible by the teacher.
- Train children in how to use the Internet.
- Ensure children have and use their own login. Reporting any new children or logins not working to LEAD IT.
- Ensure children are aware of and agree with the "Rules for Responsible Internet Use"(Appendix 1) before they grant children access to it.
- Give children clear objectives for Internet use *(e.g. structure children's access by specifying a site within which they are allowed to browse or by providing lists of suitable web sites from which the children should not stray)*.
- Preview any web sites they intend to allow children access to, to ensure the sites do not contain inappropriate material and are suitable for the age and maturity of their pupils. Be particularly mindful of images searched via Google and ensure that this is done prior to images being shared through the smart board.
- Add sites they have tested and approved to the school web site via the Website leader/ Computing leader for other teachers to use.
- Ensure that children are aware of the need to respect copyright of materials on the Internet and acknowledge the source of materials taken for use in their own work.
- Staff to complete searches through their individual logins to access appropriate material only.
- Take prompt action if they or their pupils encounter inappropriate material on the Internet. Staff to record the Uniform Resource Locator (URL) or web site address, the content of the site and any other relevant information. They must inform the Computing leader/Head Teacher as soon as possible of the site details using the forms distributed to them or extra forms located in the computer suite, (Appendix 2).
- Ensure children are shielded from unpleasant material.
- Regularly plan for and teach about online safety and share with pupils internet safety resources through the thinkuknow website, Google Legends, Purple Mash etc, to ensure their safety online. Other resources and available websites can be found, in a list, within Appendix 3.
- Take prompt action and know how to respond to a sexting incident. (see UK Council for Internet Safety for advice.)
- Understand that Upskirting is now a criminal offence and understand that police can come and talk to them if they have made a mistake or had a problem in this area.

- Take action in line with the School Anti-Bullying Policy for any cases of online bullying or cyber bullying.
- Report any incident of sexual harassment or violence (online or offline) to the DSL.
- Teach children about online reputation management (digital footprint).

Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Peer-on-peer sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.

- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy, the Child Protection and Safeguarding Policy which includes peer on peer abuse.

Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- PSHE
- ICT

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks pupils may face online are always considered when developing the curriculum.

The DSL is involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- School website
- Class Dojo

Impact

After the implementation of our robust computing curriculum, children at Meadow Farm Primary School will be digitally literate and able to join the rest of the world on its digital platform. They will be equipped, not only with the skills and knowledge to use technology effectively and for their own benefit, but more importantly – safely. The biggest impact we want on our children is that they understand the consequences of using the internet and that they are also aware of how to keep themselves safe online.

As children become more confident in their abilities in Computing, they will become more independent and key life skills such as problem-solving, logical thinking and self-evaluation become second nature.

Monitoring and review

The role of the Computing Leader

The Computing Leader is responsible for monitoring the implementation of the Online Safety Policy. The leader supports colleagues to enforce Online Safety through this policy, by giving them information about current developments and by providing a strategic lead and direction for I.T. in the school. The Computing Leader is also responsible for liaising with the Head Teacher about relevant issues and further improvement.

The role of the Data Protection Officer

Work with the DSL, head-teacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing. Ensure that all access to safeguarding data is limited as appropriate, monitored and audited.

The role of the Head Teacher

The Head Teacher has overall responsibility for the policy and its implementation; for liaison with the Governing Body, parents/carers and appropriate outside agencies and for the appointment of the Computing Leader who will have responsibility for the handling of the daily implementation of the policy.

The role of the Governing Body

The Strategic Development Committee monitors and reviews this policy on an annual basis. The committee reports its findings and recommendations to the Full Governing Body, as necessary, if the policy needs modification. The Governing Body gives consideration to any comments from parents about the Online Safety policy, and makes a record of such comments.

Policy prepared by: Doriver Lilley, Computing Lead

Date prepared: June 2026

Date ratified by the Strategic Committee: 10.06.26

Signed: (Chair of the Strategic Committee)
Mrs Melanie Gaiderman

Signed: (Head Teacher)
Mrs H Smith

Review date: June 2027

Appendix 1

Meadow Farm Primary School

Rules for Responsible Use of IT Resources in School

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign below to show that our IT online Safety rules have been understood and agreed.

Pupil Agreement
When I am using the computer or other technologies, I want to feel safe all the time. I agree that I will:

- Always keep my passwords a secret.
- Only open pages which my teacher has said are OK.
- Only work with people I know in real life.
- Tell my teacher if anything makes me feel scared or uncomfortable.
- Make sure all messages I send are polite.
- Not reply to any nasty message or anything which makes me feel uncomfortable.
- Talk to my teacher before using anything on the internet.
- Only use the internet to assist my learning, using websites that an adult has chosen or approved.
- Immediately tell an adult, and turn off my monitor if I see any webpage or receive a message I am uncomfortable with.
- Use only my own login and password, which I will keep to myself and share only with my teachers and parents.
- Only e-mail people an adult has approved and communicate in a polite and friendly manner.
- Never give out personal information or passwords.
- Not open e-mails sent by anyone I don't know.
- Not use chat rooms or social networking sites unless a specific use is approved.
- Not bring in computer games or files from home unless asked by a teacher.
- Not use digital cameras without permission.
- Not bring a mobile phone into school. If a do have to bring a mobile phone into school for safety reasons, for example I walk home alone, I will only do so with parental permission and give my phone to a member of staff for safe keeping during school hours.

I know that school may check my computer files, may monitor the sites I visit and I know that once I post a message or an item on the internet then it is completely out of my control.

Pupil Declaration

I have discussed the rules for acceptable use with an adult and I understand how to stay safe.	
Signed: My name is	**Date:**

Parent/Guardian Agreement:

- The school has installed IT equipment (computers which are connected to the internet) to help with your child's learning. The Internet Service Provider used by this school provides continually updated, filtered services to attempt to ensure only acceptable Internet sites are available.
- Your child's teacher will only set IT work which is related to the curriculum and which will benefit their learning.
- We encourage you to contact the school if you have any concerns regarding your child's use of our ICT provision, and our 'Acceptable Use Policy' is available for viewing at school and on our website.
- Portable storage devices (DVDs, memory sticks etc) from home, cannot be used in school unless they have been virus checked first.
- Occasionally digital images containing children and/or their work will be taken. Permission will be sought before these are stored or used in school.
- The computers in school can only be accessed through username and password.

In addition staff:

- Supervise children using the internet at all times.
- Check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils.
- Are extra vigilant when pupils are undertaking their own research and check that pupils are following the agreed search plan.

Parental Declaration

I have read the school's Online Safety Policy (available from school or on our website) and agree to allow my child to use the resources for the purposes described. I understand that if circumstances change before my child leaves school, it is my responsibility to inform the school.	
Signed: (Parent/carer)	**Date:**

Acceptable Use Agreement: All staff, volunteers and governors.

This covers the use of all digital technologies in school: i.e. email. Internet, network resources, learning platform, Class Dojo, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or the uses deemed 'reasonable' by the Head and the Governing Body.
- I will not reveal my password to anyone.
- I will follow good practice advice in the creation and use of my password. If my password is compromised I will ensure I chance it. I will not use anyone else's password if they reveal it to me and I will advise them to change it.
- I will not allow unauthorised individuals to access email/internet/network or other school systems, or any Local Authority systems that I have access to.
- I will ensure all documents, data etc. are printed, saved, accessed and deleted/shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email or approved communication system for any school business.
- I will only use the approved email or approved communication system with pupils or parents/carers and only communicate with them on appropriate school business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to a member of the SLT.
- I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or that are not adequately licensed.
- I will check copyright and not publish or distribute any work, including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive) to the network that does not have up-to-date anti-virus software and will keep any loaned equipment up to date using the schools recommended anti-virus and other ICT defence systems.
- I will not use personal digital cameras or camera phones or any digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images/videos and ensure I only save photographs and videos of children and staff on the staff-only drive within school.
- I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites/tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities and

that I will notify the school of any 'significant personal use', as defined by HM Revenue and Customs.

- I will ensure that any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held with the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert SLT if I feel the behaviour of any child may be a cause for concern.
- I understand that it is my duty to support a whole school safeguarding approach and wlil report any behaviour of other staff or pupils. Which I believe may be inappropriate or concerning in any way.
- I understand that all internet and network traffic/usage can be logged and this information can be made available to the Head.
- I understand that the internet encryption content (via the https protocol) may be scanned for security and/or safeguarding purposes.
- I will only use any LA system I have access to in accordance with their policies.
- Staff that have a teaching role: I will embed the school's online safety/digital literacy/counter extremism curriculum into my teaching.

I have read the school's Online Safety Policy and Acceptable Use Policy and agree to use the resources for the purposes described.	
Signed: (staff/volunteer/governor)	**Date:**

Appendix 2

Online Safety Report Form

If a child finds anything inappropriate online please record it on here and return to Mrs Lilley as soon as possible so that the website can be added to our internet block list.

Please record the URL below:

Appendix 3

Internet safety websites:

http://www.kidsmart.org.uk/
Kidsmart is an award winning practical internet safety programme website for schools, young people, parents, and agencies, produced by the children's internet charity Childnet International.

http://www.bbc.co.uk/cbbc/topics/stay-safe
This super site from the BBC has child-friendly cartoons, animations and video clips to get over the message of how to stay safe on the internet.

http://www.thinkuknow.co.uk/
Some of the videos and issues covered in this website may be more appropriate for **older children** and we would advise parents to **pre-view this site** before deciding whether to use it with your child. This website is part of the service provided by CEOP (see below). It contains lots of information on internet safety and safe surfing for young people. All hot topics about online safety are covered – including mobiles, blogging and gaming sites. Children can also tell the site if they feel uncomfortable or worried about someone they're chatting to online.

http://www.ceop.gov.uk/
This site is aimed at **parents** rather than children. CEOP is the Child Exploitation and Online Protection Centre. It is a government centre which works across the UK and maximises international links to tackle child sex abuse wherever and whenever it happens. They provide internet safety advice for parents and carers and offer a virtual police station for reporting abuse on the internet.

http://www.childnet-int.org/
This is a non-profit organisation working with others to "help make the Internet a great and safe place for children". You can download or order resources from this website. Some of the resources and on-line materials are aimed at **older children**.

http://www.chatdanger.com/
This site has hard-hitting examples of how children can be put at risk on-line and provides information about the potential dangers of interactive services like online chat, IM, online games, email and on mobiles. **We recommend that you pre-view this site before deciding to use any of the resources with your child.**

http://www.iwf.org.uk/
The "Internet Watch Foundation" provides a "hotline" in the UK for reporting illegal content on-line. If you encounter child abuse images on a website, you can report them to this site. This website also discusses the pros and cons of a number of content filtering packages, which you can use on your computer to block inappropriate material from your computer. **(This is not a website we recommend for use with your child)**