Following the introduction of the Computing curriculum in September 2014 it is the responsibility of all schools to teach e-safety. This will be through specific lessons and continuous provision, advice and support.

At Key Stage 1
Children will be taught to use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

At Key Stage 2
Children will be taught to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

E-Safety Activities and Experiences - Developing Safe Lifelong Behaviours F-Y6

The ideas here are starting points only and should be viewed as such. The suggestions could be used as a basis for developing a whole school age appropriate programme of learning for e-safety. For Starz + subscribing schools the suggestions below have been developed into ACE- a complete scheme of work with lesson ideas and resources, tasks and certification for pupils who demonstrate to adults a growing awareness and development of safe, life-long online behaviours.

Username /Password CONTACT Risk	E-safety Resources to support learning	Associated E-safety Issues
Suggested Experiences: Early experiences: To teach children that some information is precious or special because it applies just to them and that personal information is as valuable online as it is off-line, and should therefore not be shared without a parent or teacher's permission.	Looking at online identity and how others see you in an online world would be covered by all teachers prior to pupils logging-in to an online environment for the first time. Teachers should walk pupils step-by-step through the creation of personal identity profiles for use online. Return to these issues as a useful reminder or after an incident where personal security has been compromised. Also see: • For KS1 Hectors World Episode 1– Details, Details….. • Lee and Kim's Adventure - Animal Magic (Key Stage 1 - Ages 5-7) 8 minute animation • For Key Stage 2 –The SMART Crew Chapter 3 What Should you keep Safe? • ThinkUKnow 'Jigsaw' Video (8-10 year olds) • ICO Information Rights Lesson Plans 1-2	Usernames and Passwords could be shared. Username and password information is lost. Schools are encouraged to keep sensitive data such as usernames and passwords safe. Children forget to log off their computer/device.

Email CONTACT/CONDUCT Risk	E-safety Resources to support learning	Associated E-safety Issues
Suggested Experiences: Early experiences: Email collaboration alongside a responsible adult. Middle experiences Use email independently showing early understanding of the conventions and protocols of this form of communication. Later experiences: Will use email regularly to converse with peers and start to show understanding for the need to use this form of communication regularly and beyond social requirements. Show knowledge of the rules and risks when using these electronic forms of communication.	As part of your safety education talk to pupils about email etiquette and as appropriate use some of the following resources: • For younger children – Digiduck • The Adventures of The SMART crew on the **KnowItAll** website. • Spam Swatter Game • THINK on the **Cybersmart** website • Chatdanger • ICO Information Rights Lesson Plan 4 An overview of e-mail as a communication tool is given in **Cybercafe** Lesson 1. Pupils will have an opportunity to explore e-mail, via the Cybercafé web site in Lesson 2, and detailed guidance on using e-mail safely is given in Lesson 4.	Ideally, your preferred online system should support pupils as they learn the basics of emailing. Usernames and passwords may be lost, misplaced, forgotten, shared. Pupils could reveal personal details. E-mail is open to abuse such as Inappropriate content, bullying, Stalking—it is possible to be harassed with unwanted and obsessive attention via email, Viruses etc
Discussion Forums CONTACT/CONDUCT Risk	E-safety Resources to support learning	Associated E-safety Issues
Early experiences**:** Experiment with communication technologies alongside peer group. Know and can explain the differences between real and imaginary experiences. Middle experiences : Pupils are supported and encouraged to participate in any number of discussion forums within an online learning platform Later experiences: Pupils choose to participate in discussion forums within the platform on any number of issues. Know when it is appropriate to use synchronous and asynchronous forms of communication.	Agree your own set of rules for taking part in a discussion forum with reference to The **SMART** rules **Hectors World** Episode 2 -Welcome to the Carnival **Hector's World** Episode 5 Heroes THINK on the **Cybersmart** website Potential risks of chat and chat rooms are a topic of discussion in Lesson 1 of the **Cybercafé** materials. The importance of keeping personal information private, particularly in chat rooms, is covered in Lessons 3 and 6.	Personal information may be revealed. Unacceptable language or behaviour used within a forum.
Web conferencing CONTACT Risk	E-safety Resources to support learning	Associated E-safety Issues
Early experiences: Participate in a short, organised and moderated web conference with adults and peers. *Middle experiences:* Use this form of communication to exchange views or information with others showing understanding of the rules and etiquette to be followed. *Later experiences:* Pupils will use audio and video conference experiences to gather information and share work with peers and known adults.	Go to the **Flashmeeting** area on the E2bn website Under supervision, use **Facetime** or equivalent on mobile devices Link with partners across the world in an International Project	Within Cambridgeshire the preferred application is Flashmeeting- this requires initial registration by an adult plus the booking of a 'meeting' when registration is checked……all data is kept on e2bn server. Pupils should be supervised at all times. Use of unsecured systems. These systems bypass the normal filtering provided by the county and can potentially be easily accessed once registration has been completed. Conferences are unsecured and therefore safety is compromised.
Wiki Style Collaboration CONDUCT Risk	E-safety Resources to support learning	Associated E-safety Issues
Early experiences: If applicable this would be a shared whole class/group experience led by adult. Middle experiences: Experiences would be moving towards pupils becoming more independent in the use of this collaborative online tool. Activities would be directed, organised & linked to learning.	Agree your own set of rules for taking part in a wiki with reference to The **SMART** rules THINK on the **Cybersmart** website Depending on the age of the children try to set real tasks for children in the wiki. YOUtube Wikis in Plain English	Pupils should be introduced to correct etiquette. Pupils should be supervised/ wiki should be moderated by an adult. Use of unsecured systems may lead to breach of security – access to personal information etc.

Later experiences: Independent activity overseen by but not necessarily contributed to by an adult. A real experience with focussed task and outcome.

Blogging CONDUCT Risk	E-safety Resources to support learning	Associated E-safety Issues
Early experiences: Directed drawing, writing online in personal webspace. Middle experiences: More intentional diary style of writing within own personal webspace with the knowledge that this recorded journal can be viewed by peers and commented on by teacher. Later experiences: Use of personal webspace to record and reflect on personal issues with the knowledge that this can be viewed by teacher and peers.	A blog will allow individuals to make regular personal diary entries or commentaries on all manner of things maybe suggested by teachers, recording learning, descriptions of events or news with easily added paintings and graphics.	Pupils may reveal personal information or information to cause concern. Pupils should discuss the use of a Blog as a form of journal/record keeping and should know that the content can be kept private The Blog should be monitored but not necessarily 'marked' or responded to. Teachers should know the procedure if they encounter information causing concern.

Internet use CONTENT Risk	E-safety Resources to support learning	Associated E-safety Issues
Experiences for all age groups will involve exploring an online model or simulation game. Increasingly through the use of gaming type technology in schools this may be accessed through wireless handheld devices which may not include filtering and may bypass school filtering systems.	Use child friendly web based resources made instantly accessible for children and teachers to use either at home or school. See also : • Smartie the Penguin for younger children • **Hector's World** Episode 3 It's a Serious Game • **Hector's World** Episode 4 The Info Gang • **Hector's World** Episode 5 Heroes • Pupils have an opportunity to explore web browsing, via the **Cybercafé** resource, in Lesson 2. Lesson 5 tackles the issues in more depth and helps pupils to question what they see and read on web sites. • With older pupils you could work through the Kidsmart Game Page together at **http://www.kidsmart.org.uk/games/** • See Drama activity **Only A Game** Kidsmart	In school parents may object to use of internet in this way. Pupils should be supervised. Parents should be informed about school use of the internet to support learning and how activity will be monitored. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with. Pupils may encounter inappropriate material or be exposed to unnecessary advertising, dangerous websites, and abusive websites. Cambridgeshire schools use Protex filtering system supplied through E2bn or Lightspeed filtering on mobile devices.

Internet research CONTENT Risk	E-safety Resources to support learning	Associated E-safety Issues
Early experiences: Explore sources of information using menus, indexes & key words aid to search. Start to use hyperlinks/ hotspots to navigate. *Middle experiences:* Recognise and use different types of information from a range ICT based sources. Identify how different texts are organised, including on screen reference texts, magazines and leaflets. *Later experiences:* , Locate information in text on screen confidently and efficiently through using site navigational features skimming to gain overall sense of text; scanning to locate specific information; close reading to aid understanding. Know that it is important to recognise source. Know how to identify the origin of pages on the internet in order to help evaluate point of view and the author. Appraise an on screen text quickly, deciding on its value, quality or usefulness.	Third part content providers (Bug Club, Espresso, Education City) contain a range of resources for children to use without the danger of exposure to advertising features or unsuitable material. Pictures, photographs sound and video files are made available for children to explore and use to support their learning. Child-friendly search engines such as **Kidrex** are also recommended for younger age groups • Hector Protector Visit the **thinkuknow website** and install Hector Protector so that when you are searching online you always have a friend with you. See also : • **Hector's World** Episode 3 It's a Serious Game • **Hector's World** Episode 4 The Info Gang • Safe Searching Area on the Kidsmart website. • The SMART rules • Kidsmart Digital Footprints : **http://www.kidsmart.org.uk/digitalfootprints/**	Pupils may access inappropriate material in the course of their research, dangerous/misleading websites, and abusive websites. Parents may object to use of internet. Parents should be informed about school use of the internet to support learning and how activity will be monitored Pupils should be supervised. Pupils should use child friendly search engines and websites and should be directed to specific, approved on-line materials.

Social Networking CONTENT/CONTACT Risk	E-safety Resources to support learning	Associated E-safety Issues
Publishing images including photographs of pupils may happen in a variety of ways: The pupil themselves may create an avatar or online identity stamp and include a personal image. The school may publish images or video material with pupils clearly identifiable on the school website or regional broadband network Images and information may be submitted to other online sources	See: **Hectors World Episode** 1– Details, Details….. **Horrible Histories – Prudish Victorian** **Horrible Histories -Guy Fawkes**	Images and video material containing personal information may expose the pupil to strangers and safety will be compromised. Staff should be aware of relevant copyright laws. Video and photographs may enable individual pupils to be identified. File names should not refer to the pupil by name. Pupils may include personal information and images. Pupils' full names and other personal information should be omitted. Published images may breach copyright laws.
Using emerging technologies CONTENT/CONTCT/CONDUCT Risk	E-safety Resources to support learning	Associated E-safety Issues
Under supervision : Pupils may use cameras or voice recording in mobile phones/ iPods and iPads. They may Bluetooth between devices as part of their work. Schools may sanction the use of Games technology including the Wii, Sony Playstation, Microsoft Xbox etc	Use some of the following links to explore issues with your pupils: **Hector's World** Episode 5 Heroes The **CyberSmart Quiz**. **Online Do's and Don'ts** **Finding the Balance** An overview of instant messaging as a communication tool is given in Lesson 1 of **Cybercafé**. Further information is provided in Lesson 6. Lesson 2 of the **Cybercafé** encourages students to explore safe and responsible behaviours using SMS, via the website. These behaviours are further developed in Lesson 7, and are reflected upon and consolidated in Lesson 8. The importance of keeping personal information private, such as mobile telephone numbers, is covered in Lesson 3. See **Chatdanger** See **Close Encounter**	Senior management should keep use of all emerging technologies under review. Many of these devices have wireless Internet access which may not include filtering. These technologies can bypass school filtering systems and present a new route to undesirable material and communications. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means would constitute cyberbullying and therefore contravene school anti-bullying policy. Care is required in the use of any such device in school or other officially sanctioned location. Parents should be informed about school use of the devices to support learning and how activity will be monitored Parental consent should be sought.

___Produced by The ELearning Team at The ICT Service- redrafted November 2015___