CRANFORD PARK
Church Of England Primary School

E-safety Policy

UN Convention on the Right of the Child	
Article 19	You have the right to be protected from being hurt and mistreated, in body and mind

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with all other policies, in particular Anti-bullying, Equality, Teaching and Learning, PHSE, Health and

Safety, Behaviour, Allegations against Staff, Child Protection, Staff Discipline, ICT and Acceptable Use of ICT.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.
The School demonstrates that it has provided the necessary safeguards to help ensure that we have done everything that we could reasonably be expected to manage and reduce these risks. This e-safety policy explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Monitoring and Review

The implementation of this E-Safety policy will be monitored by:

- Computing Manager and Designated Safeguarding Lead
- HT
- Advisors and Inspectors

The E-Safety Policy will be reviewed regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

Incidents arising out of this policy will be dealt with according to the School's Behaviour and Anti-bullying policies. The school will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school

Headteacher:

- The Headteacher is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.
- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Computing Co-ordinator.
- The SMT are responsible for ensuring that the Computing Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

E-Safety / Computing Coordinator:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Reports regularly to Senior Management Team

Network Manager / IT Technician (HCC):

The Network Manager and ICT Technician are responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance.
- That users may only access the school's networks through a properly enforced password protection policy.
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the school Staff Acceptable Use Policy.
- They report any suspected misuse or problem to the E-Safety Co-ordinator for investigation / action / sanction.
- Digital communications with pupils (email / voice) should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other school activities.

- Pupils understand and follow the school e-safety and acceptable use policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor Computing activity in lessons, extra curricular and extended school activities.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

Designated Safeguarding Lead:

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (For KS1 it is expected that parents / carers would sign on behalf of the pupils.)
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children.

Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy
- Accessing the school website / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users:

Community Users who access school ICT systems / website will be expected to sign a Community User Acceptable Use Policy before being provided with access to school systems.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of the Computing curriculum – this covers both the use of ICT and new technologies in school and outside school. (A roadmap of what is taught in each year group each half term is attached to this policy as appendix A)
- Key e-safety messages should be reinforced as part of a planned programme of curriculum activities.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems / internet will be posted in all rooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to

ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensures that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe.)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed practice is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- An agreed practice is in place regarding the extent of personal use that users and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed practice is in place regarding the installation of programmes on school workstations / portable devices.
- An agreed practice is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school.
- Pupil's work can only be published with the permission of the pupil or parents/carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				**Pupils**			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	**x**							**x**
Use of mobile phones in lessons				**x**				**x**
Use of mobile phones in social time	**x**							**x**
Taking photos on mobile phones or other camera devices other than provided by the school				**x**				**x**
Use of hand held devices eg PDAs, PSPs	**x**							**x**
Use of personal email addresses in school, or on school network	**x**							**x**

Use of school email for personal emails		x						x
Use of social networking sites				x				x
Use of blogs outside of the School blog				x				x

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person (Headteacher) – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Unacceptable
Users shall not visit Internet sites, make, post, download, upload,	child sexual abuse images			x

data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation			x
	adult material that potentially breaches the Obscene Publications Act in the UK			x
	criminally racist material in UK			x
	pornography			x
	promotion of any kind of discrimination			x
	promotion of racial or religious hatred			x
	threatening behaviour, including promotion of physical violence or mental harm			x
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			x
Using school systems to run a private business				x
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school				x
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				x
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				x
Creating or propagating computer viruses or other harmful files				x

Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet		x	
On-line gaming (educational)	x		
On-line gaming (non educational)			x
On-line gambling			x
On-line shopping / commerce		x	
File sharing		x	
Use of social networking sites			x
Use of video broadcasting eg Youtube			x

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Such incidents will be dealt with in accordance with the School's policies particularly: Anti-bullying, Equality, Teaching and Learning, PHSE, Health and Safety, Behaviour, Allegations against Staff, Child Protection, Staff Discipline, ICT and Acceptable Use of ICT.

Policy date: April 2015

Review date: April 2019

Appendix A – E-Safety Road map for each Year Group.

E-safety road map, Year 1

UNIT	E-SAFETY COVERAGE
Unit 1.1 **We are treasure hunters**	The children learn to use simple programmable toys safely and sensibly, as well as showing respect for the work of their peers. Web access is supervised and safe practices are encouraged. Similarly, any filming is done with appropriate consent and assent.
Unit 1.2 **We are TV chefs**	The pupils learn how to use digital video cameras safely and to show respect to those they are filming, including recognising the need for consent and assent. The importance of not sharing videos more widely than is appropriate is considered, as is the need to exclude information that might identify individuals from video recordings. When using the web, pupils learn to turn the screen off and tell their teacher if they encounter material that concerns them. The pupils also start to learn about copyright, recognising that they own the copyright in their original work and that this cannot be published or copied without their permission.
Unit 1.3 **We are painters**	In searching for images on the web, pupils work initially from a set of carefully chosen sites. They again learn that they should turn the screen off and tell their teacher if they encounter material that concerns them. If work is uploaded to a public area, the importance of protecting the children's identities is recognised, as is their intellectual property rights over their original work. An extension activity provides an initial opportunity for the children to learn some aspects of using email safely.
Unit 1.4 **We are collectors**	As pupils will be working with the web and searching for images, they'll need to make sure they use this technology safely, as well as showing respect for others' intellectual property through observing copyright conditions. The pupils are taught to turn the screen off and let their teacher know if they have any concerns over content they encounter. The pupils are also introduced to the school's Acceptable Use Policy, if they haven't already had this explained to them.
Unit 1.5 **We are storytellers**	The pupils learn to use audio recorders or microphones and audio recording software safely and sensibly. The pupils need to be aware of copyright material, and show appropriate respect for the owners of intellectual property when using technology. Regard is shown for appropriate consent and assent, school policies and third party terms and conditions if the pupils' stories are uploaded to external websites.
Unit 1.6 **We are celebrating**	The pupils have an opportunity to search for images on the web, and again learn to use technology safely, switching off the screen if they have concerns, and reporting these to their teacher. The pupils are taught to respect the copyright conditions associated with any third party images they use. Pupils only use photos of themselves if appropriate permission is in place. If children share their work, then attention is paid to protecting their identity and copyright. If they send cards by email they use a class address and consider some aspects of using email safely.

You may photocopy this page to share with parents.
To see how e-safety is covered in other year groups, see the CD-ROM.

E-safety road map, Year 2

UNIT	E-SAFETY COVERAGE
Unit 2.1 **We are astronauts**	The pupils must let their teacher know if they encounter inappropriate material when they search the web. If the pupils use third-party images in their projects, they should use images with public domain or Creative Commons licences. The pupils may upload their projects to the Scratch website, if they have registered for accounts using a parent's e-mail address. They learn to observe MIT's terms and condition.
Unit 2.2 **We are games testers**	There are concerns about the violent nature of some games. Choosing games wisely, including observing PEGI age restrictions and playing in moderation, are aspects of the safe and respectful use of technology that pupils learn about in this unit. As in Unit 2.1, the pupils may upload their projects to the Scratch website, if they have registered for accounts using a parent's e-mail address. Comments on the Scratch website are not moderated before they appear, although the pupils can report any which are inappropriate. This provides an opportunity to learn about where to go for help and support when they have concerns about content or contact.
Unit 2.3 **We are photographers**	The children learn that once images are posted online, it's impossible to control what happens to them. Facial recognition software and geotagging mean that those posting images might inadvertently fail to keep some personal information private. The children learn how to minimise these risks, and learn what they should do if they have concerns about images they encounter on the web. The children also learn about what is acceptable and unacceptable to photograph, for example, that it is usually not a good idea to take or share photographs in which children can be identified, or that might reflect badly on the school.
Unit 2.4 **We are researchers**	The pupils consider how to stay safe while researching online, and show respect for others' ideas and intellectual property by citing their sources, and using licensed images. Safe search filters are in place for using Google or Bing and school internet access is filtered.
Unit 2.5 **We are detectives**	The pupils learn about some of the risks associated with email. They learn that attached files can contain viruses or other harmful programs, that email addresses and embedded links can be 'spoofed', and that 'spam' is a common problem. It is recommended that all emails are sent and received via a single class email address. The password for this account is not shared with children. If the children do use individual accounts, they'll need to keep their account details private and share their email address only with people they know and trust.
Unit 2.6 **We are zoologists**	The pupils again learn that when sharing photographs and geo-location information online they need to consider the importance of keeping personal information private; they achieve this by not including names or photographs of people. The pupils are taught to respect rules for using digital equipment when out of the classroom, to ensure the equipment is kept safe and that they are not so focused on using it that they become unaware of risks around them.

You may photocopy this page to share with parents.
To see how e-safety is covered in other year groups, see the CD-ROM.

E-safety road map, Year 3

UNIT	E-SAFETY COVERAGE
Unit 3.1 **We are programmers**	The pupils need to consider copyright when sourcing images for their programs and/or uploading their own work to the Scratch community site. Searching for content for programs or viewing others' cartoons also offers an opportunity to develop safe search habits. If the pupils participate in the Scratch community, they need to think about what information they can share and how to participate positively in an online community, as well as obtaining parental permission.
Unit 3.2 **We are bug fixers**	The pupils could consider the implications of bugs in software. Participating in the Scratch community would enable the pupils to help others with their projects as well as allowing them to receive help on their own. Participation requires parental permission, and the pupils should consider what behaviour is acceptable online.
Unit 3.3 **We are presenters**	In filming one another, the pupils need to ensure that the appropriate permission has been obtained, and that they act respectfully and responsibly when filming, editing and presenting their work. The pupils should think through the implications of videos being made available on the school network or more widely via the internet. They should discuss why schools and other organisations have strict policies over filming.
Unit 3.4 **We are network engineers**	The pupils learn about how networks, including the Internet, operate. They learn that data transmitted via the internet is not always encrypted. They consider some of the implications for privacy, e.g. their 'digital footprint' associated with using the internet. They become aware of the importance of DNS for safe use of the internet. They learn to use command line diagnostic tools safely and responsibly.
Unit 3.5 **We are communicators**	The pupils should think about the safe use of email. They learn how email can be used positively. They become aware of some of its risks, including malware attachments, hacked accounts, spam and spoofed links, but also learn how their exposure to such risks can be reduced. They consider the importance of introductions in extending circles of trust. They learn how video conferencing can be used positively, to support learning with a known partner.
Unit 3.6 **We are opinion pollsters**	The pupils learn some of the legal and ethical requirements for designing online surveys and processing data. They also consider what information it would be appropriate for them to give in an online survey, and some implications of data processing. The pupils can use online tools for collaborating on survey design and analysis, considering how to use these appropriately. The survey itself could address issues of the pupils' attitudes to online safety.

You may photocopy this page to share with parents.
To see how e-safety is covered in other year groups, see the CD-ROM.

E-safety road map, Year 4

UNIT	E-SAFETY COVERAGE
Unit 4.1 **We are software developers**	The pupils need to consider copyright when sourcing images or media for their programs and/or uploading their own work to the Scratch community site. Searching for content for their programs or viewing others' games also offers an opportunity to develop safe search habits. If the pupils participate in the Scratch community, they need to think about what information they can share and how to participate positively in an online community, as well as obtaining parental permission.
Unit 4.2 **We are toy designers**	The pupils again need to think carefully about copyright in sourcing images and other media for their toy prototypes and presentations, or if uploading their own work to the Scratch community. If the pupils do participate in the online Scratch community, they should think through how to do so in a safe and responsible manner, and should obtain their parents' consent. If the pupils link their programs to hardware, they need to take care to work safely with a range of tools and electronic equipment.
Unit 4.3 **We are musicians**	The pupils need to think about copyright when sourcing audio or publishing their own compositions. They are encouraged to use Creative Commons licensed content if working with others' audio files. There's an opportunity to discuss how copyright relates to music performed in school as well as illegal downloading and sharing of copyrighted music.
Unit 4.4 **We are HTML editors**	The pupils learn how easy it is to create content for the web. The unit provides an opportunity to address some of the risks of using the web, and how pupils could best keep themselves safe while doing so. They learn how easily web pages can be modified, which provides an opportunity to consider the reliability of web-based content.
Unit 4.5 **We are co-authors**	The pupils learn about Wikipedia, considering some strategies for evaluating the reliability of online content as well as the rules and processes that the Wikipedia community has evolved. The pupils develop a shared wiki, thinking carefully about how to do so safely and responsibly, and considering what conduct is appropriate when collaborating on a shared resource.
Unit 4.6 **We are meteorologists**	The pupils consider the importance of obtaining and using accurate data for any information-processing work. If the pupils film one another, they need to ensure appropriate permission is obtained and that recordings are made, edited and shown in safe, respectful and responsible ways. The pupils should think carefully about the implications of uploading their films to the school network or to the internet.

You may photocopy this page to share with parents.
To see how e-safety is covered in other year groups, see the CD-ROM.

E-safety road map, Year 5

UNIT	E-SAFETY COVERAGE
Unit 5.1 **We are game developers**	The pupils need to consider copyright when sourcing images or media for their games and/or uploading their own work to the Scratch community site. Searching for content for their games or viewing others' games also offers an opportunity to develop safe search habits. If the pupils participate in the Scratch community, they need to think about what information they can share and how to participate positively in an online community, as well as obtaining parental permission. The pupils might also consider some personal implications of playing games, perhaps including violent computer games.
Unit 5.2 **We are cryptographers**	The pupils learn how information can be communicated in secret over open channels, including the internet, using cryptography. They learn about the public key system used to sign and encrypt content on the web, and how they can check the security certificates of encrypted websites. They learn about the importance of password security for online identity and consider what makes a secure password.
Unit 5.3 **We are artists**	The unit provides an opportunity to reinforce messages around safe searching and evaluating the quality of online content. If the pupils upload their work for others to see, they should consider the importance of protecting personal information as well as recognising that they are sharing their own copyrighted work with an audience.
Unit 5.4 **We are web developers**	E-safety forms the focus of this unit, with the pupils working collaboratively to develop a website in which they present their own authoritative content on a broad range of issues around the safe and responsible use of technology. In doing so, they consider the reliability and bias of online content, how to contribute positively to a shared resource, and how to use search engines safely and effectively.
Unit 5.5 **We are bloggers**	The pupils write content for their own or a shared blog, thinking carefully about what can be appropriately shared online. They consider issues of copyright and digital footprint as well as what constitutes acceptable behaviour when commenting on others' blog posts. The pupils also think about the importance of creating high-quality online content and become more discerning in evaluating content as they review others' blogs. If the pupils' blogs are publicly accessible, it is important that any comments are moderated by their teacher; it is worth discussing with the pupils why the comments should be moderated.
Unit 5.6 **We are architects**	The pupils should observe good practice when searching for and selecting digital content. If the pupils choose to locate their 3D models geographically, they should avoid sharing private information. The pupils should think about copyright when adding content to their model or publishing images or videos of their model.

You may photocopy this page to share with parents.
To see how e-safety is covered in other year groups, see the CD-ROM.

E-safety road map, Year 6

UNIT	E-SAFETY COVERAGE
Unit 6.1 **We are app planners**	The pupils consider the capabilities of smartphones and tablet computers, and how these can be used purposefully. They become aware of some of the capabilities of these devices, including how they can be used to record and share location information; they consider some of the implications of this. They use search engines safely and effectively. The pupils could make use of their own tablets or smartphones in school, considering how they can do this safely and to good effect.
Unit 6.2 **We are project managers**	The pupils use online tools safely and effectively, considering how they can contribute positively to a shared project. Again, they use search engines safely and effectively. They may also make use of online content, respecting any copyright conditions.
Unit 6.3 **We are market researchers**	The pupils show regard for the ethical and legal frameworks around conducting interviews and online surveys, such as the need to preserve anonymity and/or confidentiality. In conducting their research, the pupils need to act safely and responsibly, as well as showing respect for those participating in the research.
Unit 6.4 **We are interface designers**	The pupils need to think carefully about copyright in relation to both sourcing and creating their own digital content and user interface components for their apps.
Unit 6.5 **We are app developers**	Pupils using their own or the school's tablets or smartphones for this unit need to consider how to do so safely and purposefully. Children participating in online communities for either of the development platforms here need to do so in a safe, responsible and respectful manner. The pupils should also think carefully about any safety implications of the apps they develop.
Unit 6.6 **We are marketers**	In marketing their app, the pupils should consider the legal and ethical frameworks around advertising across different media. They should also think about the need to protect personal information about themselves and other members of their group when marketing their app. In creating websites for their apps, the pupils need to consider the e-safety implications for the site's users as well as themselves.

You may photocopy this page to share with parents.
To see how e-safety is covered in other year groups, see the CD-ROM.