Gusford Primary School

e-Safety and Acceptable Use Policy 2014

Introduction

As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children's Act 2004, it is the duty of school/education setting or other establishments to ensure that children and young people are protected from potential harm both within and beyond the school/education setting or other establishment environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies.

Aims

This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'e-Safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school/education setting or other establishment .
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school/education setting or other establishment.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Roles and Responsibilities

Governors & Headteacher

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of e-Safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:

- The Headteacher has a designated e-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of who takes this role within the school/education setting or other establishment.
- Time and resources is provided for the e-Safety Lead and staff to be trained and update policies, where appropriate.
- The Headteacher/e-Safety Lead is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Headteacher will inform the Governors at the Curriculum meetings about the progress of or any updates to the e-Safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to safeguarding. At the Full Governor meetings, all Governors will be made aware of e-Safety developments from the Curriculum meetings.
- The Governors **MUST** ensure e-Safety is covered within an awareness of safeguarding and how it is being addressed within the school. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded.
- An e-Safety Governor (can be the ICT or Safeguarding Governor) will ensure the school has an Acceptable Use Policy (AUP) in place, with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:

  Challenging the school about having:

  - Firewalls.
  - Anti-virus and anti-spyware software.
  - Filters.
  - Using an accredited ISP (internet Service Provider).

    - Awareness of wireless technology issues.
    - A clear policy on using personal devices.
- Ensure that any misuse or incident is dealt with appropriately, according to policy and procedures, (see the Managing Allegations Procedure on Suffolk Local Safeguarding Children's Board website) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police or involving parents/carers.

Local e-Safety Lead

It is the role of the designated e-Safety Lead to:

- Appreciate the importance of e-Safety within the school and to recognise that Gusford Primary has a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the school.
- Ensure that the AUP is reviewed annually, with up-to-date information and that training is available for all staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops and the learning platform *or ensure the technician is informed and carries out work as directed*.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher on a regular basis.
- Liaise with the PSHE, safeguarding and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct e-Safety information can be taught or adhered to.
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified, in accordance with the Suffolk Safeguarding Children Board Allegations made Against Staff in Education Settings to ensure the correct procedures are used with incidents of misuse.
- Work alongside the technician, to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised Refer to the Managing Allegations Procedure, SSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure there is regular monitoring of internal e-mails, where:
    - Blanket e-mails are discouraged
    - Tone of e-mails is in keeping with all other methods of communication
- Report overuse of blanket e-mails or inappropriate tones to the Headteacher and/or Governors.

Staff or Adults

It is the responsibility of all adults within the school to:

- Ensure that they know who the Senior Designated Person for Safeguarding is within school/education setting or other establishment, so that any misuse or incidents can be reported which involve a child.
- Where an allegation is made against a member of staff it should be reported immediately to the Headteacher/Senior Designated Person.

In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately.

- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Headteacher/Senior Designated Person immediately, who should then follow the Managing Allegations Procedure, where appropriate.
- Report any concerns regarding filtering levels to the e-Safety Lead.
- Alert the e-Safety Lead of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign an Acceptable Use Statement to show that they agree with and accept the agreement for staff using non-personal equipment, within and beyond the school, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- To ensure that School bursars follow the correct procedures for any data required to be taken from the premises.
- Report accidental access to inappropriate materials to the e-Safety Lead in order that inappropriate sites are added to the restricted list or controlled with the Local Control options via your broadband connection.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school/education setting or other establishment's network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the Gusford accident/incident reporting procedure in the same way as for other non-physical assaults e.g. Reported on Pupil Asset, if persistent or significant then logged on Gusford Incident Form (details will be inputted onto Handsam).

Children and Young People

Children and young people should be:

- Involved in the review of Acceptable Use Agreement in line with this policy being reviewed and updated.
- Responsible for following the Acceptable Use Agreement whilst within the school setting as agreed at the beginning of each academic year or whenever a new child attends the school for the first time.
- Taught to use the internet in a safe and responsible manner through ICT, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

Appropriate and Inappropriate Use by Staff or Adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

All staff will receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they will sign to be kept under file with a signed copy returned to the member of staff.

The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

Please refer to appendices for a complete list of Acceptable Agreement for Staff.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

By Children or Young People

Acceptable Use Agreements and the letter for children, young people and parents/carers are outlined in the Appendices. These detail how children and young people are expected to use the internet and other technologies within the school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The agreement will be on display within the classrooms, computer suite and near stand alone PCs.

School/education setting or other establishments should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school/education setting or other establishment that the agreement are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school/education setting or other establishment.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond the school environment.

Communications

	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	✓						✓	
Use of mobile phones in lessons		✓						✓
Use of mobile phones in social time	✓							✓
Taking photos on personal mobile phones			✓*					✓
Taking photos on personal camera devices			✓*					
Use of hand held devices e.g. iPads	✓					✓		
Use of personal email addresses in school, or on school network	✓							✓
Use of school email for personal emails				✓				✓
Use of chat rooms / facilities		✓					✓	
Use of instant messaging		✓						✓
Use of social networking sites		✓						✓
Use of blogs	✓				✓			

* with permission from the Headteacher following guidance outlined in this policy

Inappropriate use

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	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				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LGfL and / or the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
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					✓	
On-line gaming (educational/non educational)			✓			
On-line gambling					✓	
On-line shopping / commerce				✓		
File sharing		✓				
Use of social networking sites				✓		
Use of video broadcasting e.g. Youtube		✓				

In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at school/education setting or other establishment, the following consequences should occur

- Any child found to be misusing the internet by not following the Acceptable Use Agreement will have a letter sent home to parents/carers explaining the reason for suspending the child use for a particular lesson or activity.
- Further misuse of the agreement will result in not being allowed to access the internet for a period of time and a meeting arranged with parents/carers to discuss the matter.
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to minimise the window so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies will be addressed by the e-Safety Lead/Headteacher.

Children will be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

The Curriculum and Tools for Learning

Internet Use

Children will be how to use the Internet safely and responsibly, through ICT and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies will have been taught by the time they leave *Year 6*:

- Internet literacy.
- Making good judgements about websites and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- Knowledge of copyright and plagiarism issues.
- File sharing and downloading illegal content.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.

These skills and competencies are taught within the curriculum so that children and young people have the security to explore how online technologies can be used effectively, but in a safe and responsible manner. Children and young people will know how to deal with any incidents with confidence.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- Full name (first name is acceptable, without a photograph).
- Address.
- Telephone number.
- E-mail address.
- School/education setting or other establishment.
- Clubs attended and where.
- Age or DOB.
- Names of parents.
- Routes to and from school/education setting or other establishment.
- Identifying information, e.g. I am number 8 in the school/education setting or other establishment Football Team.

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Images of children and young people should be stored according to policy.

Pupils with Additional Learning Needs

Gusford Primary School provides access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-Safety awareness sessions and internet access.

Website

The uploading of images to the school website should be subject to the same acceptable agreement as uploading to any personal online space. Permission will be sought from the parent/carer prior to the uploading of any images. Settings will consider which information is relevant to share with the general public on a website.

External Websites

In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, they are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

E-mail Use

E-mail addresses for children and young people to use, as a class and/or as individuals are part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

Individual email accounts can be traced if there is an incident of misuse whereas class email accounts cannot, especially for older users.

Staff, children and young people should use their school issued email addresses for any communication between home and school only. A breach of this may be considered a misuse.
All staff school issued email addresses will include a standard disclaimer stating that the views expressed are not necessarily those of the Active Learning Trust.

Parents/carers are encouraged to be involved with the monitoring of emails sent, although the best approach with children and young people is to communicate about who they may be talking to and assess risks together.

Teachers are expected to monitor their class use of emails where there are communications between home and school.

Mobile Phones and Other Emerging Technologies

Children may bring their mobile phone into school, however, it will be locked in the school safe when the child arrives and given back to the child at the end of the school day.

(I) Personal Mobile Devices

Staff are allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people under any circumstances.**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
- Staff should be aware that games consoles such as the Sony Playstation, Microsoft Xbox, Nintendo Wii and DSi and other such systems have Internet access which may not include filtering. Before use within school, authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.
- The school is not responsible for any theft, loss or damage of any personal mobile device.

(ii) School Issued Mobile Devices

The management of the use of these devices is similar to those stated above, but with the following additions:

- Where the establishment has provided a mobile device to a member of staff, such as a laptop, PDA or mobile phone, only this equipment should be used to conduct school business outside of the school building.

The children will be taught to understand the use of a public domain and the consequences of misuse. Relevant curriculum links will be made to highlight the legal implications and the involvement of law enforcement. Other technologies which the school use with children and young people include:

. Photocopiers.
. Fax machines.
. Telephones.
. iPads

Video and Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

When in school there is access to:

- Digital cameras
- Flip cameras
- iPads

Group photographs are preferable to individual children and should not be of any compromising positions or in inappropriate clothing. Photos taken on personal cameras and phones must be with the Headteacher's permission and downloaded onto a piece of school equipment e.g. laptop, network, or deleted within 2 weeks of being taken. Photos taken of children should be saved onto the school network. However, members of staff may have photos of children within documents stored on their laptops

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to the school website. Photographs should not include the child's first name.

The sharing of photographs via weblogs, forums or any other means online will only occur after permission has been given by a parent/carer or member of staff.

Managing Social Networking and Other Web Technologies

All staff sign a Social Network Policy (Appendix 6).
Social Networks, with the exception of Twitter to allow access for the school account, are blocked by the internet filter.

Social Networking Advice for Staff

Social networking outside of work hours, on non school issue equipment, is the personal choice of all staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. See Social Network Policy for guidelines and advice given to staff. (see Appendix 6)

Safeguarding Measures – Filtering

Gusford Primary school uses a Draytek 2920 Router/Firewall with Web Content Filtering. Web-based content is filtered by the 3C Technology Ltd broadband connection with age appropriate settings. Changes can be made to the filtering levels through contact with 3C Technology Ltd.

Anti-virus and anti-spyware software is used on all network and stand alone PCs or laptops and is updated on a regular basis.

A firewall ensures information about children and young people and the school cannot be accessed by unauthorised users.

Children will use a search engine that is age appropriate such as AskJeeveskids or Yahooligans.

Links or feeds to e-Safety websites are provided.

Tools for Bypassing Filtering

Pupils and staff are forbidden to use any technology designed to circumvent, avoid or bypass any school/education setting or other establishment security controls (including internet filters, antivirus solutions or firewalls) as stated in the Acceptable Use Agreement.

Violation of this rule will result in disciplinary or in some circumstances legal action. Please refer to the 'Staff Procedures Following Misuse by Staff/Children and Young People' sections of this document.

Note: Block banning of student's ICT or internet access can be severely disruptive to learning across the curriculum and can also affect lesson planning and should only be applied in the most serious breaches.

Monitoring

The e-Safety Lead/School Technician will monitor the use of online technologies by children and staff, on a regular basis. Network Managers do not have overall control of network monitoring.

Teachers will monitor the use of the Internet during lessons and also the use of e-mails from school and home, on a regular basis.

Computers around the school

All computers are protected in line with the network.
Where software is used that requires a child login, this is password protected so that the child is only able to access themselves as a user. Children and young people are taught not to share passwords.
The same acceptable use agreement applies for any staff and children and young people using this technology, this will is displayed in all areas a computer is used.

Parents – Roles

Each child will receive a copy of the Acceptable Use Agreement on an annual basis or first-time entry to the school which needs to be read with the parent/carer, signed and returned to school, confirming both an understanding and acceptance of the agreement.

It is expected that parents/carers will explain and discuss the agreement with their child, where appropriate, so that they are clearly understood and accepted. The school will keep a record of the signed forms.

Support

As part of our approach to developing e-Safety awareness with children and young people, the school will offer parents the opportunity to find out more about how they can support the school in keeping their child safe and find out what they can do to continue to keep them safe whilst using online technologies beyond our school. The school wants to promote a positive attitude to using the World Wide Web and therefore wants parents to support their child's learning and understanding of how to use online technologies safely and responsibly.
We will do this by holding an e-Safety Parent/Carer Information Evenings once per annum.

Providing parents with information on how the school protects children and young people whilst using the learning platform facilities, such as the Internet and E-mail. It will also be an opportunity to explore how the school is teaching children and young people to be safe and responsible Internet users and how this can be extended to use beyond the school environment.

Links to Other Policies - Behaviour and Anti-Bullying Policies

Please refer to the Behaviour and Anti-Bullying Policy for the procedures in dealing with any potential bullying incidents via any online communication, such as mobile phones, e-mail or blogs.

Managing Allegations against Adults Who Work With Children and Young People

Please refer to the Managing Allegation Procedure, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the Senior Designated Person (SDP) for safeguarding within the school immediately. In the event of an allegation being made against a Head teacher, the Chair of Governors should be notified immediately.

Local Authority Designated Officer (LADO) - Managing Allegations:

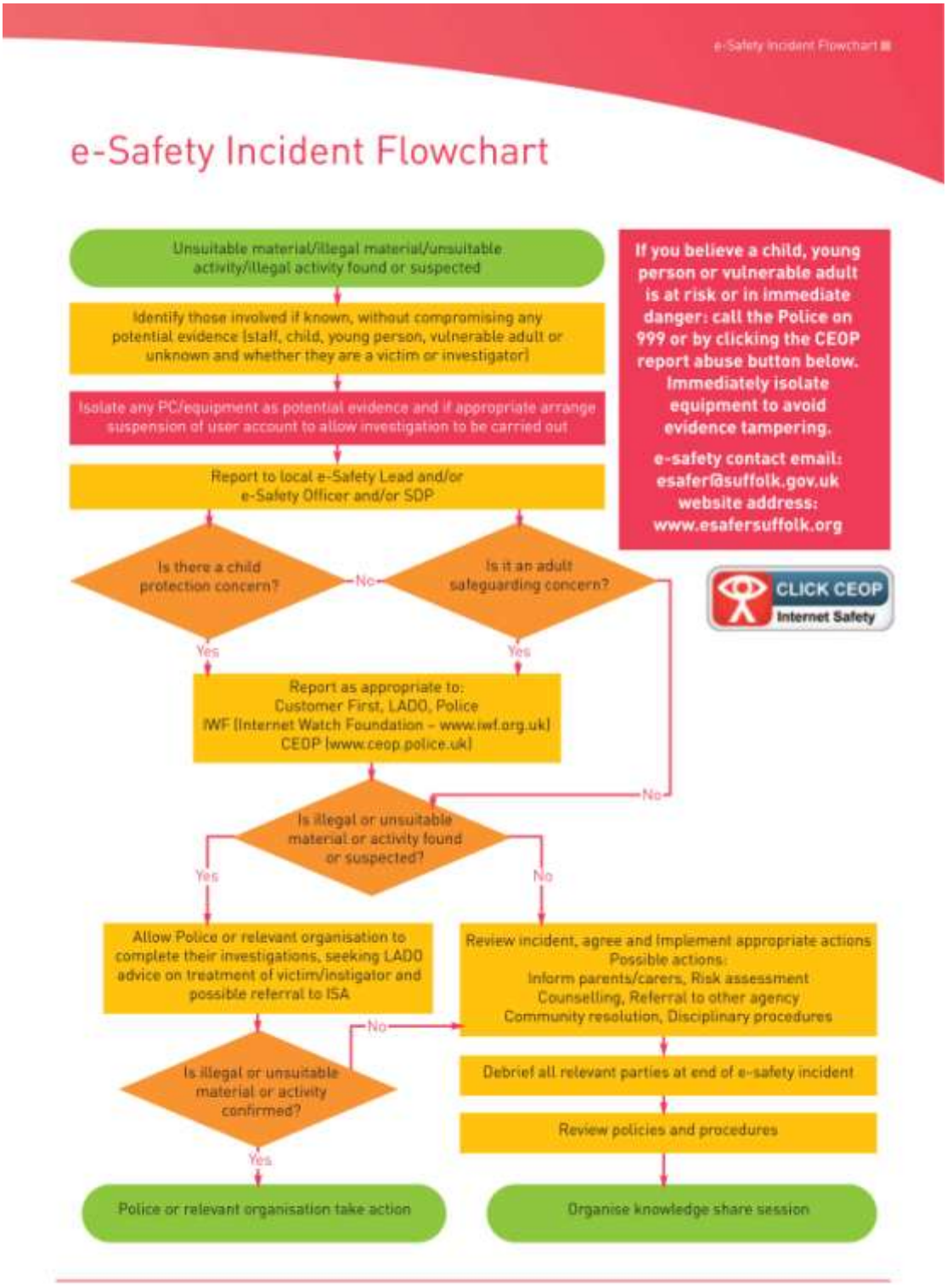
The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

Disciplinary Procedure for All School/Education Setting or Other Establishment Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Curriculum Development

The teaching and learning of e-Safety is embedded within the PSHE and Computing curriculum (see Appendix 8: Switched On Computing e-Safety Road Map) to ensure that the key safety messages about engaging with people are the same whether children and young people are on or off line.
A SCC Learning Together workshop for Year 6 Primary children is annual and part of the PSHE curriculum for raising awareness on staying safe and being responsible.


e-Safety Incident Flowchart
e-Safety Incident Flowchart
Unsuitable material/illegal material/unsuitable activity/illegal activity found or suspected
Identify those involved if known, without compromising any potential evidence (staff, child, young person, vulnerable adult or unknown and whether they are a victim or investigator)
Isolate any PC/equipment as potential evidence and if appropriate arrange suspension of user account to allow investigation to be carried out
Report to local e-Safety Lead and/or e-Safety Officer and/or SDP
Is there a child protection concern?
No
Is it an adult safeguarding concern?
Yes
Yes
Report as appropriate to:
Customer First, LADO, Police
IWF (Internet Watch Foundation – www.iwf.org.uk)
CEOP (www.ceop.police.uk)
No
Is illegal or unsuitable material or activity found or suspected?
Yes
No
Allow Police or relevant organisation to complete their investigations, seeking LADO advice on treatment of victim/instigator and possible referral to ISA
Review incident, agree and implement appropriate actions
Possible actions:
Inform parents/carers, Risk assessment
Counselling, Referral to other agency
Community resolution, Disciplinary procedures
No
Is illegal or unsuitable material or activity confirmed?
Debrief all relevant parties at end of e-safety incident
Review policies and procedures
Yes
Police or relevant organisation take action
Organise knowledge share session
If you believe a child, young person or vulnerable adult is at risk or in immediate danger: call the Police on 999 or by clicking the CEOP report abuse button below. Immediately isolate equipment to avoid evidence tampering.
e-safety contact email: esafer@suffolk.gov.uk
website address: www.esafersuffolk.org
CLICK CEOP
Internet Safety

Appendix 2

Acceptable Use Agreement for Staff and Governors

This agreement applies to all online use and to anything that may be downloaded or printed.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Headteacher, Senior Designated Person or e-Safety Lead in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Senior Designated Person is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail. I know I should use my Gusford e-mail address and phones (if provided) and only to a child's Gusford e-mail address upon agreed Gusford use.
- I know that I must not use the school system for personal use unless this has been agreed by the Headteacher and/or e-Safety Lead.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Lead prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-Safety issues and procedures that I should follow.

I have read, understood and agree with these Agreement as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed…….Date…….

Name (printed)…….

Appendix 3

Acceptable Use Agreement for Visitors

This agreement applies to all online use and to anything that may be downloaded or printed.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Headteacher, Senior Designated Person or e-Safety Lead in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Senior Designated Person is.
- I know that I must not use the school system for personal use unless this has been agreed by the Headteacher and/or e-Safety Lead.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Lead prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software on a non-Gusford issued device which I have permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been given a copy of the Responsible Internet and Digital Technologies use document so I am clear on the procedures that I should follow.

I have read, understood and agree with these Agreement as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed…….Date…….

Name (printed)…….

Responsible Internet and Digital Technologies use

Written: March 2014
Review date: March 2015

Communications

	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	✓						✓	
Use of mobile phones in lessons		✓						✓
Use of mobile phones in social time	✓							✓
Taking photos on personal mobile phones			✓*					✓
Taking photos on personal camera devices			✓*					
Use of hand held devices e.g. iPads	✓					✓		
Use of personal email addresses in school, or on school network	✓							✓
Use of school email for personal emails				✓				✓
Use of chat rooms / facilities		✓					✓	
Use of instant messaging		✓						✓
Use of social networking sites		✓						✓
Use of blogs	✓				✓			

* with permission from the Headteacher following guidance outlined in the e-Safety and Acceptable Use policy

Inappropriate use

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	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				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LGfL and / or the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
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					✓	
On-line gaming (educational/non educational)			✓			
On-line gambling					✓	
On-line shopping / commerce				✓		
File sharing		✓				
Use of social networking sites				✓		
Use of video broadcasting e.g. Youtube		✓				

My e-Safety Agreement

This is my agreement for using the internet safely and responsibly.

- I will use the internet to help me learn.
- I will learn how to use the internet safely and responsibly.
- I will only send email messages that are polite and friendly.
- I will only email, chat to or video-conference people I know in the real world or that a trusted adult has approved.
- Adults are aware when I use online tools such as video conferencing.
- I agree never to give out passwords or personal information like my full name, address or phone numbers.
- I agree never to post photographs or video clips without permission or that I will not include my full name with photographs.
- If I need help I know who I can ask and that I can go to www.thinkuknow.co.uk for help if I cannot talk to a trusted adult.
- If I see anything on the internet that makes me feel uncomfortable, I know what to do.
- If I receive a message sent by someone I don't know, I know what to do.
- I know I should follow these guidelines as part of the agreement with my parent/carer.
- I agree to look after myself and others by using my internet in a safe and responsible way.

Signed..... Dated.....

Name.....(Printed)

Appendix 6

Gusford Primary School

"Promoting Achievement and Success."

Staff Social Networking Policy

Person Responsible: Headteacher – C Tapscott
Policy Review: May 2013
Next Review: May 2015

Introduction

Social Networking through internet sites such as FaceBook has become more and more popular over the last few years. The vast majority of staff at Gusford now have FaceBook accounts. Many parents and many children, some as young as 7, also have accounts.

A number of problems have occurred in Suffolk schools recently where staff have inadvertently made a comment or posted a photo/video that has led to parental complaints. This puts the governors and senior managers in the school in a very difficult position and the member of staff may face disciplinary action for unprofessional conduct. The following list of Dos and Don'ts is an attempt to protect staff from such action.

DO

- Select your "friends" carefully and consider who is able to see your profile – remember that friends of your friends may sit with them at a computer or may be given access without you knowing.
- Limit access to your profile to only your "friends"; ensure that your privacy settings are always up to date – the social networking providers change the setup of these frequently.
- Update privacy settings every 3 months to avoid default settings being used by the social network group resetting your privacy settings.
- Ensure that the privacy settings on your photo albums are set to "friends only".
- Ensure comments/photos/videos of yourself that may be posted by you or others do not show you or other members of staff in a way that could be construed as unprofessional for a member of staff/volunteer working in a school.
- Consider carefully the "groups" that you may join and are then shown on your profile.
- Use language that is appropriate as a member of Gusford.
- Consider carefully comments made on any social network medium will reflect on you and the school

DO NOT

- Accept children (under the age of 18) that you have met/taught in the course of your profession as "friends".
- Upload photos/videos of school activities that involve children or jeopardise the professional status of others.
- Post any comments of any nature about children and/or parents in the school.
- Post any comments or pictures about staff or school activities

Please note that privacy and security settings are not guaranteed and that anything you post may become in the public domain. Any breach of the above may result in disciplinary action.

Name: Signed: Date

Appendix 7

Gusford e-Safety Incident Report

Details of all e-Safety incidents must be reported to the e-Safety Coordinator.
When incidents involve Cyberbullying this document should copied and attached to the Bullying Incident form.

Date and time:
Name of pupil or staff member: Year:
Male or Female:
Room and computer/device number:
Details of incident (including evidence):
Actions:

Incident reported by:

Position:

Date:

E-safety road map, Year 1

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.

.

E-safety road map, Year 2

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.

E-safety road map, Year 3

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.

E-safety road map, Year 4

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.

E-safety road map, Year 5

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

.

E-safety road map, Year 6

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.