St Francis' Primary School

E-Safety Policy

Policy Updated: December 2015
Review Date: September 2018

E Safety Policy

Rationale

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

The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

E-Safety covers issues relating to children, as well as adults, and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care', which applies to everyone working with children. The staff receive annual Safeguarding training which includes 'Prevent' training to ensure they are aware of issues surrounding radicalisation and extremism and how to deal with them and Child Sexual Exploitation (CSE) awareness information.

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
- Unauthorized 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 other school policies (e.g. Behaviour, Anti-bullying, Child Protection and Safeguarding policies, Health and Safety, Home School Agreement and Staff Code of Conduct).

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.

Background

Schools must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. Schools must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to

report any concerns. All members of staff need to be aware of the importance of good E-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Schedule for Development, Monitoring and Review

The implementation of this e-safety policy will be monitored by the: E-*Safety Coordinator, Senior Leadership Team, Computing Technician.*

Monitoring will take place at once a year.

The Governing Body will receive a report on the implementation of the E-Safety Policy generated by the monitoring group (which will include anonymous details of e-safety incidents) once a year.

The E-Safety Policy will be reviewed annually, or more 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.

The next anticipated review date will be: September 2018.

Should serious e-safety incidents take place, the following external persons / agencies should be informed: LA IT Manager, LA Safeguarding Officer, Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students / pupils (e.g. Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
  - parents / carers
  - staff

Policy approved by Head Teacher: …… Date: ……

Policy approved by Governing Body: ……..….. Date: ……
(Chair of Governors)

Scope of the Policy

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 IT 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 (see Anti Cyber Bullying Policy), or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy (and associated behaviour and anti-bullying policies) and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Curriculum Committee* receiving regular information about e-safety incidents and monitoring reports.
The *E-Safety Governor* is Mirella O'Donoghue.

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- 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 E-Safety Co-ordinator.
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Co=ordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

- The Headteacher and another member of the Senior Leadership should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Co-ordinators:

The School E-Safety Co-ordinators are Maria Wheeler, Lorna Dommett and Claire Mills.

- lead the e-safety committee
- take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority
- liaise with technical staff
- receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments
- meet regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attend relevant meeting / committee of Governors
- report regularly to Senior Leadership Team

Technical Staff:

The Technician is 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 the Security Policy and Acceptable Usage Policy and 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, in which passwords are regularly changed
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- 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

Teaching and Support Staff

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 students / pupils 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 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
- in lessons where internet use is pre-planned 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

Designated Safeguarding Lead

The DSL 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

E-Safety Committee

Members of the E-Safety committee will assist the E-Safety Co-ordinator with:

- the production, review and monitoring of the school e-safety policy / documents.

The E-safety committee members are:

- E-Safety Co-ordinator – Claire Mills
- Computer technician – Marillia Soares
- Headteacher – Maria Wheeler
- Deputy head – Nanda Fawcett
- Inclusion leader – Lorna Dommett

Pupils:

- are responsible for using the school systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 and 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 new technologies than

their children. The school will therefore take opportunities to help parents understand these issues through *parents' evenings, newsletters, website and information about national / local e-safety campaigns / literature.*

Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website in accordance with the relevant school Acceptable Use Policy.

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 will be provided as part of Personal Social Health and Citizenship Education (PHSCE) and should be regularly revisited – this will cover both the use of IT and new technologies in school and outside school
- key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral 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 Acceptable Use Policy (AUP) and encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school
- staff should act as good role models in their use of IT, the internet and mobile devices
- the school fosters a 'No Blame' environment that encourages pupils to tell a teacher or adult immediately if they encounter any material that makes them feel uncomfortable
- ensures pupils know what to do if they find inappropriate web material

Education – Parents / Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- newsletters
- the school web site
- a partnership approach to e-Safety at home and at school with parents' evenings with demonstrations and suggestions for safe home Internet use

- the school prospectus
- parents will be requested to sign an E–Safety/Internet agreement as part of the Registration Document when their child starts school and when their child enters KS2.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children

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:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- 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 Co-ordinator will receive regular updates through attendance at LA training sessions and by reviewing guidance documents released by BECTA / LA and others.
- This E-Safety Policy and its updates will be presented to and discussed by staff in INSET days.
- The E-Safety Co-ordinator will provide advice, guidance or training to individuals as required

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in IT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.
- Participation in school training / information sessions for staff or parents

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 IT systems will be managed in ways that ensure that the school meets the e-safety technical requirements and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school IT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee.
- All users will be provided with a username and password by the technician who will keep an up to date record of users and their usernames.
- The “master / administrator” passwords for the school IT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. 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.
- The school broadband is maintained and supports the managed filtering service provided by Unicorn
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher
- Any filtering issues should be reported immediately to Claire Mills or Maria Wheeler
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
- School IT technical staff regularly monitor and record the activity of users on the school IT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users' activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager
- 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.
- There is provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- staff must speak to the computer technician in order to install programmes onto school workstations/portable devices
- Staff must ensure that encrypted memory sticks are used for sensitive data and that these memory sticks are checked regularly for virus protection
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot 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 technology 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

- 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.
- Pupils will use age-appropriate tools to research Internet content.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.
- The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

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 e.g. 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 website (may be covered as part of the AUP signed by parents or carers at the start of the year)

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.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

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	✓					Y5 Y6			
Use of mobile phones in lessons		✓[1]						✓	
Use of mobile phones in social time	✓							✓	
Taking photos on personal mobile phones or other				✓				✓	

camera devices									
Use of hand held devices e.g. tablets		✓				✓			
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		✓					✓		

1 School trips or emergency situations

* In accordance with AUP

- 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. Pupils may only use approved email accounts for school purposes.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – 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. Staff will only use official school provided email accounts to communicate with pupils and parents/carers
- Whole class or group email addresses will be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use when available, if not they will also use class email addresses.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.

School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.
Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.

Pupils Use of Personal Devices

• If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
• If a pupil needs to contact his/her parents/carers they will contact the school office. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
• Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

• Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
• Staff will be issued with a school phone where contact with pupils or parents/carers is required.
• Mobile Phone and devices will be switched off, Bluetooth communication should be switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by the Headteacher or Deputy Head Teacher in emergency circumstances. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times
• If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
• Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
• If a member of staff breaches the school policy then disciplinary action may be taken.

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, 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 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)		✓		
On-line gaming (non-educational)				✓

On-line gambling			✓
On-line shopping / commerce		✓1	
File sharing		*✓2	
Use of social networking sites		*✓3	
Use of video broadcasting e.g. Youtube		*✓4	

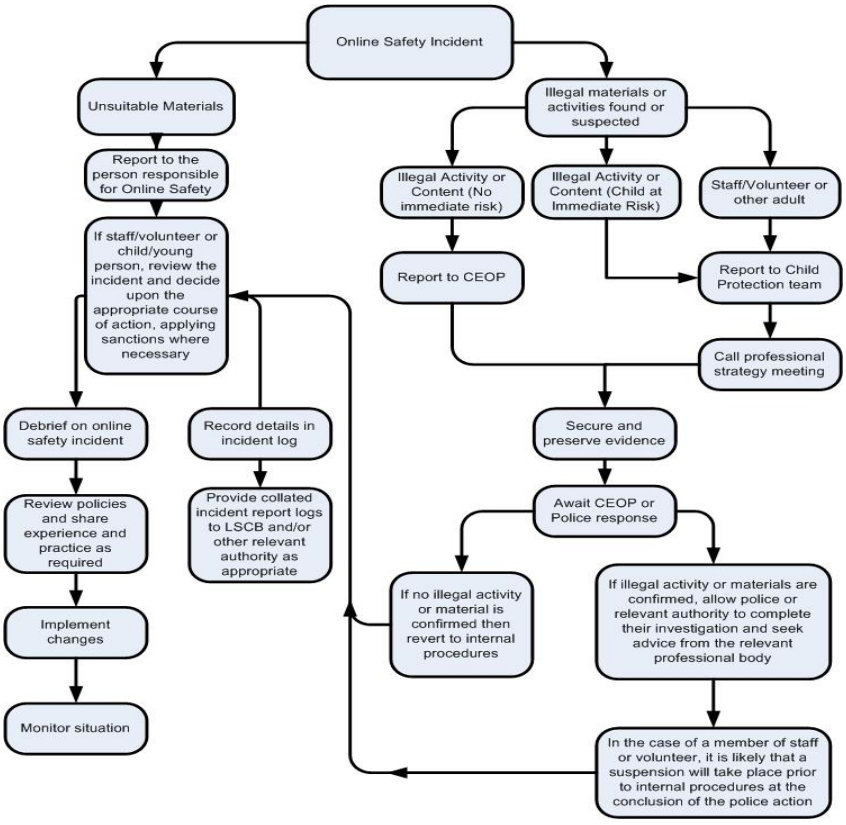
1 See Financial responsibility policy
2 See Data Protection Act
3 For educational purposes
4 For educational purposes

Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of IT, 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. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.
- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The flow chart below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. Staff are issued with the ‘What to do if...?’ guide on safety issues (Appendix 1) It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures detailed on page 16.

Incidents will be recorded using a log based on the NSPCC ‘Keeping Children Safe Online’ E-Safety Incident Log. (See Appendix 1)

Pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓		✓		✓
Unauthorised use of non-educational sites during lessons	✓						✓
Unauthorised use of mobile phone / digital camera / other handheld device		✓			✓		
Unauthorised use of social networking / instant messaging / personal email	✓				✓		✓

Unauthorised downloading or uploading of files	✓			✓			✓
Allowing others to access school network by sharing username and passwords							
Attempting to access or accessing the school network, using another student's / pupil's account		✓			✓	✓	
Attempting to access or accessing the school network, using the account of a member of staff		✓			✓		✓
Corrupting or destroying the data of other users	✓						✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓			✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓				✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓			✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓		✓		✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓						
Deliberately accessing or trying to access offensive or pornographic material		✓			✓		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓						

Staff Actions / Sanctions

Incidents:	Refer to Senior Leader	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓							
Unauthorised downloading or uploading of files	✓				✓			
Allowing others to access school network by		✓			✓			

sharing username and passwords or attempting to access or accessing the school network, using another person's account								
Careless use of personal data eg holding or transferring data in an insecure manner		✓			✓			
Deliberate actions to breach data protection or network security rules		✓			✓			✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓						
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓						✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		✓						
Actions which could compromise the staff member's professional standing	✓							
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓						✓
Using proxy sites or other means to subvert the school's filtering system		✓			✓			
Accidentally accessing offensive or pornographic material and failing to report the incident	✓							
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓				
Breaching copyright or licensing regulations	✓							
Continued infringements of the above, following previous warnings or sanctions		✓						✓

Appendices

1. What to do if...? Guide for Teachers

To be given to all staff as reference material.
(Includes a copy of the NSPCC 'Keeping Children Safe Online' E-Safety Incident Log.)

2. Staff and Volunteers Acceptable Use Policy

To be signed by all staff upon starting at St. Francis'.
To be signed by all volunteers/teaching practice and work experience students, etc., with access to school computer systems.
One copy to be retained by staff member.
One copy to be placed in staff file.

3. Pupil Acceptable Use Policy KS1

4. Pupil Acceptable Use Policy KS2

5. Cover Letter to Parent/Carer – AUP for KS1/KS2 Agreement

6. Parent /Carer Acceptable Usage Policy Agreement

To be given to all parents/carers when their child starts at St Francis'

7. Digital and Video Images

8. Legislation

9. Links to Other Organisations or Documents

10. Resources

Appendix 1

What to do if...?

A Reference Guide for Staff

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety coordinator and decide whether to inform parents of any children who viewed the site.
3. Inform the school technician and ensure the site is filtered

An inappropriate website is accessed <u>intentionally</u> by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technician and ensure the site is filtered if need be.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
   - Remove the PC to a secure place.
   - Instigate an audit of all IT equipment by the schools IT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (contact Personnel/Human Resources).
   - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police or High Tech Crime Unit and follow their advice.
   - If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety, anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.

8. Inform the LA e-safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA e-safety officer.

The school may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA e-safety officer.
6. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher and e-safety coordinator.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

St. Francis' Primary School - E-Safety Incident Log

(Based on the format recommended by the NSPCC and CEOP through the 'Keep children safe online' training materials)

Details of incident	
Time	
Date	
Where did the incident occur?	
Name and contact details of person reporting incident	
Who was involved in the incident?	☐ Child / young person ☐ Staff member ☐ Other (please specify)
Names and contact details of those involved	
Type of incident	Please tick: • Bullying or harassment • Online bullying or harassment (cyberbullying) • Sexting (self-taken indecent imagery • Deliberately bypassing security or access • Hacking or virus propagation • Racist, sexist, homophobic, religious hate material • Terrorist material • Other (please specify)

Description of incident	
Nature of incident	☐ deliberate access ☐ accidental access
Did the incident involve material being	Please tick: • Created • Viewed • Printed • Shown to other • Transmitted to others • Distributed
Could this incident be considered as	Please tick: • Harassment • Grooming • Cyberbullying • Sexting (self-taken indecent imagery)
Action taken	**Staff** Please tick: • Incident reported to head teacher / senior management • Advice sought from children's social care • Incident reported to police • Incident reported to CEOP • Incident reported to Internet Watch Foundation

	• Incident reported to IT technician • Disciplinary action to be taken • E-Safety Policy to be reviewed/amended **<u>Child/Young Person</u>** Please tick: • Incident reported to member of staff (specify) _____ • Incident reported to social networking site • Incident reported to IT technician • Child's parents informed • Disciplinary action to be taken • Child/young person debriefed • E-Safety Policy to be reviewed/amended

Outcome of Incident/Investigation	
Children's Social Care	
Police/CEOP	
Organisation	
Individual (staff member/child/young person)	
Other (HR, legal etc.)	
Learning from the case	
Key learning point 1	
Key learning point 2	
Key learning point 3	
Recommendations and timescales to implement	
Recommendation 1	
Recommendation 2	
Recommendation 3	

Signed		Print name Date	

Signed		Print name Date	
Signed		Print name Date	
Signed		Print name Date	

Appendix 2

Acceptable Use Policy - Staff Agreement Form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will log off the network when leaving a workstation unattended.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system for any school business.
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the E Safety Co-ordinator.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other IT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I understand that when using any social networking I am required to uphold the reputation of the school, maintain reasonable standards in my behaviour and uphold the public trust in the profession. I will not do anything that will bring the school into disrepute.

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will access school resources remotely only through the school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching, including on-line safety/digital literacy and counter extremism.
- I will encourage pupils to report issues that arise.
- I will alert the school's named child protection officer if I feel the behaviour of any child I teach may be a cause for concern.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage and network usage can be logged and this information could be made available to the SLT on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

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

Full Name ..... (printed)

Job title .....

Head Teacher

M. Wheeler

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

- *Further information is available at the CEOP, NSPCC and ThinkuKnow websites.*
- *Relevant legislation can be found in the school's E-Safety Policy,*

Appendix 3

Pupil Acceptable Use Policy KS1

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that *pupils* will have good access to IT to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

To be read, discussed and signed with a parent/carer on entry to the school.

To be stored in the children's individual records folders.

Copy of poster to be displayed in classroom.

St. Francis Catholic Primary Caterham

"For it is in giving that we receive."
- St. Francis of Assisi

KS1 Acceptable Use Agreement

Think before you click

S 	I will only use the Internet and email with an adult
A 	I will only click on icons and links when I know they are safe
F 	I will only send friendly and polite messages
E 	If I see something I don't like on a screen, I will always tell an adult

My Name: My Signature:

Appendix 4

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that *pupils* will have good access to IT to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

To be read, discussed and signed with a parent/carer on entry to KS2 at St Francis' Primary School.

To be stored in the children's individual records folders.

Copy of poster to be displayed in classroom.

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

Do we need

Appendix 5

Cover Letter to Parent/Carer – AUP for KS1/KS2 Agreement

Appendix 6

Parent/Carer Acceptable Use Policy Agreement

"For it is in giving that we receive."
- St. Francis of Assisi

Parent/Carer Acceptable Use Policy Agreement

The Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

(For detailed information on keeping children safe online, please visit www.ceop.gov.uk/ and www.thinkuknow.co.uk/ . To see the school's e-safety policy, please visit the school's website.)

The school will try to ensure that pupils will have good access to Computing to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carer's Name

Pupil Name

As the parent / carer of the above *pupil*, I give permission for my son / daughter to have access to the internet at school and the school's email system, IT systems and equipment.

I have supported my child in signing an Acceptable Use Agreement and know they will receive e-safety education to help them understand the importance of safe use of IT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the IT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed

Date

Head Teacher

M. Wheeler

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

Appendix 7

Use of Digital/Video Images

See the School's General Permission Form

Appendix 8

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of

conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Appendix 9

Links to Other Organisations or Documents

The following links may help those who are developing or reviewing a school e-safety policy.

Child Exploitation and Online Protection Centre (CEOP)
http://www.ceop.gov.uk/

ThinkUKnow
http://www.thinkuknow.co.uk/

CHILDNET
http://www.childnet-int.org/

INSAFE
http://www.saferinternet.org/ww/en/pub/insafe/index.htm

BYRON REVIEW ("Safer Children in a Digital World")
http://www.dcsf.gov.uk/byronreview/

Becta
Website e-safety section - http://schools.becta.org.uk/index.php?section=is
Developing whole school policies to support effective practice:
http://publications.becta.org.uk/display.cfm?resID=25934&page=1835
Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:
http://publications.becta.org.uk/display.cfm?resID=32422&page=1835
"Safeguarding Children in a Digital World"
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_tl_rs_03&rid=13344

LONDON GRID FOR LEARNING
http://cms.lgfl.net/web/lgfl/365

KENT NGfL
http://www.kented.org.uk/ngfl/ict/safety.htm

NORTHERN GRID
http://www.northerngrid.org/ngflwebsite/esafety_server/home.asp

SOUTH WEST GRID FOR LEARNING:
"SWGfL Safe" - http://www.swgfl.org.uk/safety/default.asp

NATIONAL EDUCATION NETWORK
NEN E-Safety Audit Tool: http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html

CYBER-BULLYING

DCSF - Cyberbullying guidance
http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=spectrum&ProductId=DCSF-00658-2007

Teachernet
http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/

Teachernet "Safe to Learn – embedding anti-bullying work in schools"
http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

East Sussex Council – Cyberbullying - A Guide for Schools:
https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx

References to other relevant anti-bullying organisations can be found in the appendix to the DCSF publication "Safe to Learn" (see above)

SOCIAL NETWORKING

Home Office Task Force - Social Networking Guidance -
http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

Digizen – "Young People and Social Networking Services":
http://www.digizen.org.uk/socialnetworking/

Ofcom Report:
http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

MOBILE TECHNOLOGIES

"How mobile phones help learning in secondary schools":
http://partners.becta.org.uk/index.php?section=rh&catcode=_re_rp_02_a&rid=15482

Mobile phones and cameras:
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_mob_03

DATA PROTECTION AND INFORMATION HANDLING

Information Commissioners Office - Data Protection:
http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

BECTA - Data Protection:
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_dp_03

PARENTS GUIDES TO NEW TECHNOLOGIES AND SOCIAL NETWORKING:
http://www.iab.ie/

Appendix 10

Resources

http://www.swgfl.org.uk/safety/safetyresources.asp?page=schoolst_resources&audienceid=3

Links to other resource providers:
BBC Chatguides: http://www.bbc.co.uk/chatguide/index.shtml

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

NCH - http://www.stoptextbully.com/

Chatdanger - http://www.chatdanger.com/

Internet Watch Foundation: http://www.iwf.org.uk/media/literature.htm

Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx

London Grid for Learning: http://cms.lgfl.net/web/lgfl/safety/resources