Shottery St Andrew's C.E Primary School E Safety Policy

Pupils interact with the Internet and other communications technologies such as mobile phones on a daily basis and experience a wide range of opportunities, attitudes and situations. Anyone can send messages, discuss ideas and publish material with little restriction, with identities also hidden. The exchange of ideas and social interaction are both greatly beneficial but can also place young people in danger. E-safety comprises all aspects relating to children and young people and their safe use of these technologies, both in and out of school. It includes the need to educate children and young people about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences, it is part of the 'Duty of Care' which applies to everyone working with children.

The world of electronic communication is fast changing, it includes but it not restricted to social networking sites and blogs, Internet research: web sites, search engines and Web browsers, Mobile phones and Tablets, Internet communications: e-Mail and instant messaging (IM), Webcams and videoconferencing, Games consoles and MP3 players.

The school recognises that technology plays an important and positive role in children's lives, both educationally and socially. It is committed to helping all members of the school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly.

Risks include receiving inappropriate content, predation and grooming, requests for personal information, bullying and threats, publishing inappropriate content, publishing personal information; identity theft; hacking and security breaches

There must be a balance between controlling access, setting rules and educating students for responsible use. The responsibility for this is shared by pupils, school staff, ICTDS support structures and parents themselves who should support pupils to understand safe and responsible ICT use. It is important that children and young people are made aware of appropriate behaviour in relation to contacting others and they must also understand that publishing personal information could compromise their security. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. We aim to ensure that the skills for safe use taught within school will be transferred to the home environment.

Many primary pupils have access to mobile devices. The use of handhelds and Internet-enabled devices both inside and outside school is increasing rapidly. The most ICT capable may be the most vulnerable. Children who interact poorly socially may be more at risk from inappropriate online contact. **In order to support the e-safety of pupils a copy of this policy will be placed on the school's website and will be emailed annually to parents and governors.**

Pupils need to learn safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. They need to understand that rules given to them must be followed and that as they get older that certain rules may change and develop. Pupils need to learn how to apply strategies that will help them to avoid certain "risks" and to deal with situations which may arise. Since most safety principles rely on children being able to explain what happened or to ask for help children with severe learning difficulties must be given particular support. Childnet have produced a range of materials to support pupils with special educational needs: http://www.childnet-int.org/kia/sen/.

Development ,Monitoring and Review of this Policy

This e-safety policy has been developed by the all teaching staff at our school, parents have been consulted and the policy has been approved by Governors.

By adopting the principles within this policy, Shottery Primary aims to demonstrate that reasonable steps have been taken to protect pupils. The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT and for child protection. The Designated Lead for Child Protection is Mrs Sarah Marshall. The school is registered for the 360° E Safety mark and is committed to achieving the necessary requirements for 360° Accreditation. Due to the fast changing nature of these technologies, this policy will be reviewed annually. An annual e-safety week will be held to remind children (at an age appropriate level) as to the dangers associated with the internet and issues directly related to the school's internet policy. Related Policies: PSHE, Anti-Bullying, Behaviour, Data protection, Safeguarding, Computing, ICT policy.

Scope of the Policy

This policy applies to all members of the Shottery St Andrew's School community (including staff, students/ pupils, volunteers, parents/ carers, visitors) who have access to and are users of school's ICT systems, both in and out of the school.

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 site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school / academy, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching, for and of, electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Shottery St Andrew's CE Primary 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.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences of Internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly. The Headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

Roles and Responsibilities

The trust between pupils and school staff is essential to education but occasionally breaks down. This is not new, but has been highlighted by better awareness of human failings and greater respect for children. The Child Exploitation and Online Protection centre (CEOP) has been set up by the Home Office to "safeguard children's online experiences and relentlessly track down and prosecute offenders". At Shottery Primary the expectations upon for behaviour and usage of users of our computing facilities are set out in our Acceptable Use Policies and detail amongst others requirement for passwords, privacy and appropriate language.

Headteacher

The Headteacher, Mrs Sarah Marshall has a duty of care for ensuring the safety (including e-safety) of members of the school community, including the monthly monitoring of e-safety forensic reports, these reports are stored in the Headteacher's Email Account. All staff 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. The Headteacher is responsible for ensuring that relevant staff receive suitable training to enable them to carry out roles with respect to e-safety

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 Resources Committee receiving regular information about e-safety incidents and monitoring reports. David Pashley in his capacity as Designated Governor for Safeguarding will monitor E safety within the school through regular meetings with the DSL.

ICT Coordinator

The ICT Co ordinator, is Louise Cooper who works alongside the E safety Co ordinator, Helen Howlett who leads the e-safety committee and takes day to day responsibility for e-safety issues which includes a leading role in establishing and reviewing the school e-safety policies/ documents. Alongside the Headteacher and DSL the ICT Coordinator and E safety coordinators provide training and advice for staff and liaises with the Local Authority and relevant technical support staff.

Designated Safeguarding Lead

The DSL should be trained in e-safety issues and be aware of the potential for serious child protection and safeguarding issues which may arise from: sharing of personal data , access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.

Teaching and Support Staff

Staff should act as good role models in their use of digital technologies the internet and mobile devices.

Staff are responsible for ensuring that they have an up to date awareness of e-safety matters, e-safety policy and practices at Shottery St Andrew's CE Primary. All Shottery Primary staff will be given the School e-Safety Policy and are expected to sign the Acceptable ICT Use Agreement . In signing, staff should be aware that Internet traffic is monitored by Policy Central and can be traced to the individual user, staff should ensure they do not allow anyone to use their log in and should ensure they log out at the end of a session. Professional conduct is essential, Staff accept that these measures are to help ensure staff and pupil safety. A member of staff who flouts IT security advice, or uses email or the Web for inappropriate reasons risks dismissal.

Any allegation of inappropriate behaviour by anyone using the Internet should be reported to the Headteacher. Allegations against members of staff will need to be investigated using the recommended WCC procedures and HR informed.

Email, text messaging and IM (Instant Messenger) all provide additional channels of communication between staff and pupils and inappropriate behaviour can occur. Staff should realise the power of the technology in Police hands to identify the sender of inappropriate messages. Staff are advised against having open/unprotected social networking pages, where they do they should be aware of the dangers of pasting inappropriate pictures or of allowing pupils to become 'friends'. **All digital communications with pupils and parents should be on a professional level** and only carried out using official school systems via the admin3057 address. In lessons where internet use is pre-planned students / 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.

Pupils

Pupils are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy so that they learn to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. E-safety issues are embedded in all aspects of the curriculum and other activities and pupils understand and follow the e-safety and acceptable use policies. They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

Parents / Carers

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way, yet many parents and carers have only a limited understanding of e-safety risks and issues. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. At Shottery St Andrew's CE Primary we will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and information about national/ local e-safety campaigns/ literature. Parents and carers will be encouraged to support the school / academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and Portal

The school regards e-safety as a wider community issue and confirms that it will deal rigorously with out of school e-safety incidents that relate to members of the school community.

Why use the Internet?

Internet use is a part of the statutory curriculum and a necessary tool for staff in support teaching and pupils to enhance learning. The internet is used to support the school's management information including pupil assessment and business administration systems. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

The internet provides access to world-wide educational resources including museums and art galleries

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Alongside safeguarding E safety will form part of the standard weekly staffmeeting agenda as well as a standard element of the first INSET day training in September. 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 Agreements.

Using the Internet to Support Learning

Parental permission is required for internet use. The school maintains a current record of all staff and pupils who are granted Internet access. **All users must read and abide by the 'Acceptable ICT Use Policy' before using any school ICT resource. At Key Stage 1, parents will be asked to read and acknowledge the school's 'Acceptable ICT Use Policy'.**

Most Internet use in school is safe, purposeful and beneficial to learners and pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. However there is always an element of risk: even an innocent search can occasionally turn up links to adult content or violent imagery.

For the youngest pupils, the greatest risk is through inadvertent access. Fast broadband means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content. At Shottery Primary our agreed procedure is to close or minimise the page immediately. If pupils have seen the page, teachers will talk to them about what has happened, and reassure them.

Good planning and preparation is critical in ensuring a safe starting point for the development of Web search skills and strategies. If the aim is to teach search skills, BBC Schools offers a safe environment. The search box automatically restricts the search to the BBC Schools site. Importantly, primary pupils can learn skills such as keyword selection to narrow down searches, and evaluating quality and relevance. Care should be taken when using search engines such as Google and strict filtering must applied. Go to www.google.co.uk and click Preferences. Image searches are especially risky. There are some safer areas for searching for images such as: www.pics4learning.com and www.dorlingkindersley-uk.co.uk/static/cs/uk/11/clipart/. For most other curriculum-related research, sites such as Kidrex, Yahooligans and **Ask Jeeves for Kids** offer suitable services and are available as shortcuts in the Internet folder of Pupil Programs. These avoid the need to use an unfenced search engine.

Rules for Internet access will be posted in all networked rooms and pupils will be informed that Internet use will be monitored. E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: A planned e-safety curriculum should be provided as part of Computing lessons and should be regularly revisited. Key e-safety messages should be reinforced as part of a planned programme of assemblies and pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided that not everything we read online is true. Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Email

E-mail is an essential means of communication for both staff and pupils. Staff and pupils have email accounts provided through the Warwickshire Learning Platform for all school communications. Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Whilst school staff may use the school facilities to access their private email accounts they should be aware that in the school context, e-mail should not be considered private and will be monitored through Policy Central who will detect the use of 'banned words' used in e-mail. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and staff, and the preservation of human rights, both of which are covered by recent legislation.

All users should be expected to adhere to the generally accepted rules of network etiquette (netiquette):

Be polite.

Use appropriate language.

Do not get abusive in your messages to others.

Do not reveal the personal address, phone number or other personal details of yourself or other users.

Do not arrange to meet anyone without specific permission.

Do not use the network in such a way that would disrupt the use of the network by other users.

Illegal activities are strictly forbidden.

Note that e-mail is not guaranteed to be private.

System administrators have access to all mail.

Messages relating to or in support of illegal activities may be reported to the authorities.

Web Cams, Iris Connect and Video Conferencing

Pupils should ask permission from the supervising teacher before using web cams. All videoconferencing should be supervisedby the class teacher and should take place within the classroom. When recording a lesson using Iris Connect the video should only be uploaded to the secure website and should only be used for professional development and monitoring purposes. Any videoconferencing / web cams in classrooms must be switched off when not in use and not set to auto answer.

The school Web site

The school is mindful of the information it publishes on its website and takes all reasonable steps to ensure that personal security is not compromised. Photographs of a pupil should not be published without the parent's or carer's written permission. Photographs of children will never be published alongside full names and the contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

Use of digital and video images

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, parents and pupils need to be aware of the risks associated with publishing digital images

on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

- **When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, parents will be requested not to publish photographs of other people's children on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers 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 wherever possible only be taken on school equipment, where the personal equipment of staff is used, for example to upload images onto the school twitter account, the images should be removed as soon as possible to minimise the risk of images being accidentally uploaded onto home computers.
- 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 students / 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 in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Managing Information Services: Technical – infrastructure / equipment, filtering and monitoring

At Shottery St Andrew's we work in partnership with the Warwickshire ICT Development Service (ICTDS). The school uses the Warwickshire Broadband with its firewall and filters which allows only approved internet traffic. There are also filters in place, which help to prevent inappropriate material from entering the network. No filtering system is totally effective. Where staff or pupils discover unsuitable sites, the URL, time and date must be reported to the ICT coordinator who will ask the office Manager to inform ICTDS .The school provides an addition level of protection through its deployment of Impero and Policy Central in partnership with Warwickshire ICT Development Service which monitors text appearing on the screen and keyboard input, identifying the use of any words that are included in the application's list of 'banned words'. The software captures the screen and identifies the machine and user details. The image is then recorded in a central location and forensic reports sent monthly to the Headteacher. The school also purchases technical support through WES and ensures virus protection is installed and updated regularly.

All teaching staff and pupils must use their own accounts when using school devices to enable effective monitoring to support this all staff are issued with passwords, pupils in KeyStage 2 are also issued with passwords. The school ICT systems will be reviewed regularly with regard to security. Virus protection will be installed and updated regularly by the LA. The ICT subject leader supported by the school technician will ensure that the system has the capacity to take increased traffic caused by Internet use.

Bring Your Own Device (BYOD)

At Present pupils are not able to bring electronic devices to school, with the exception of e readers and mobile phones for pupils walking home alone in Class 1. Mobile Phones must be handed in to the office on arrival at school. Pupils bringing e readers to school which have access to the Internet will not be given access to the school's secure network.

Staff are permitted to link their own devices to the school's wireless network but must ensure they follow the acceptable use policy. Staff should not answer texts or phonecalls within lessons and phones should be set on silent. Personal phones must not be used to record images of pupils.

Protecting personal data

The quantity and variety of data held on pupils, families and on staff is expanding quite quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify an individual). The act also gives rights to the people the information is about i.e. the right of subject access, lets individuals find out what information is held about them.

The eight principles are that personal data must be:

Processed fairly and lawfully;

Processed for specified purposes;

Adequate, relevant and not excessive;

Accurate and up-to-date;

Held no longer than is necessary;

Processed in line with individuals rights;

Kept secure;

Transferred only to other countries with suitable security measures.

At Shottery Primary Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Staff must ensure that they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. Staff should only use personal data on private devices and should not use public computers. Memory sticks with personal data must be encrypted.

Social Networking

Shottery St Andrew's CE Primary School has a duty of care to provide a safe learning environment for pupils and staff. Social networking sites and newsgroups will be blocked unless a specific use is approved. Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc…

Where school staff become aware that pupils are accessing inappropriate social media sites they will inform parents that this is taking place.

School staff should ensure that no reference should be made in personal social media accounts to pupils, parents the school or its staff. School staff are advised to ensure they have the appropriate privacy settings in place when using social media and not to enable school parents or pupils to have access to their site/ account.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / academy and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

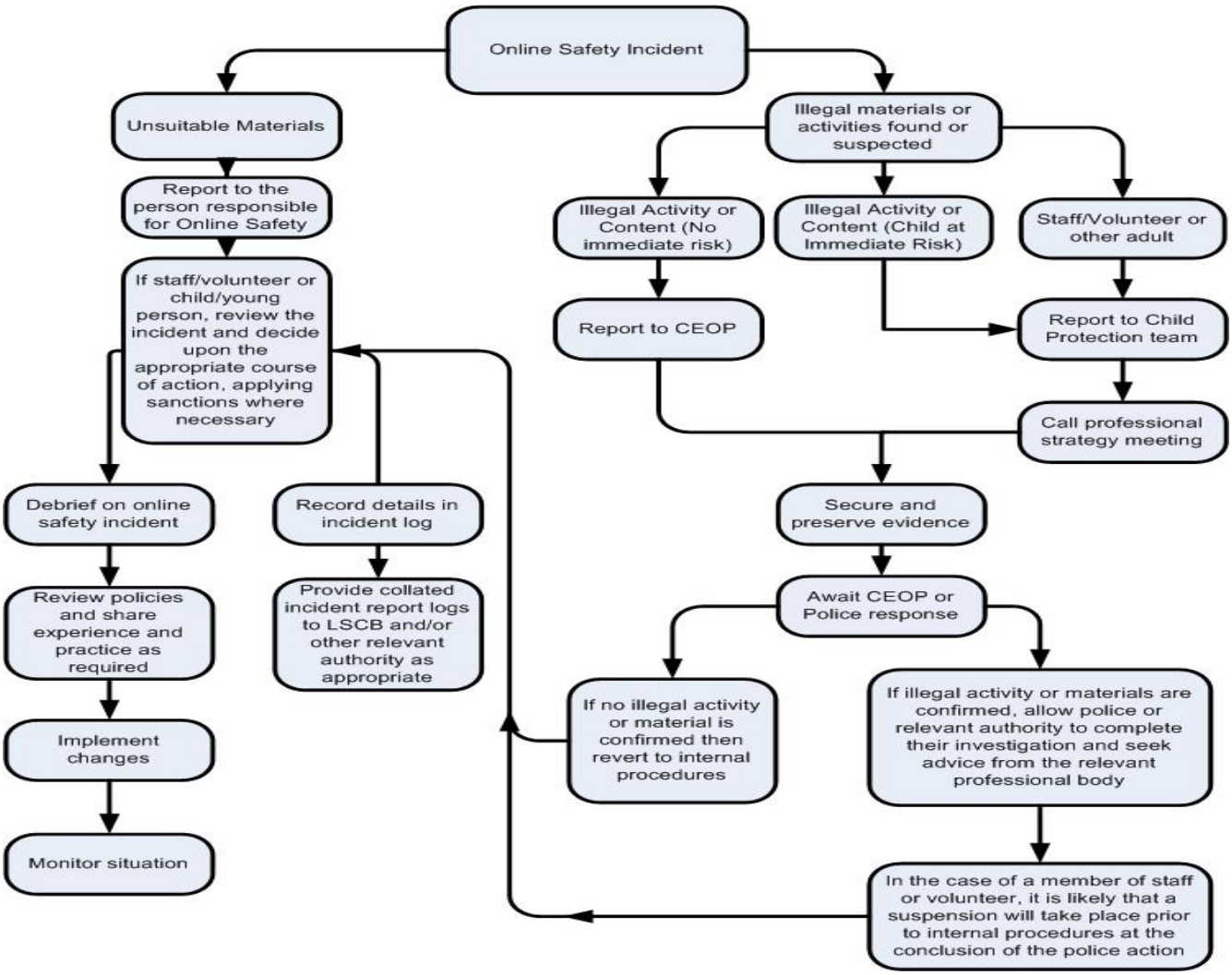
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					x
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					x
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					x
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					x
	pornography				x	
	promotion of any kind of discrimination				x	
	threatening behaviour, including promotion of physical violence or mental harm				x	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				x	
Using school systems to run a private business					x	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					x	
Infringing copyright					x	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, network access codes and passwords)					x	
Creating or propagating computer viruses or other harmful files					x	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					x	
On-line gaming (educational)						
On-line gaming (non educational)						
On-line gambling						
On-line shopping /banking						
File sharing						
Use of social media						

Use of messaging apps					
Use of video broadcasting eg Youtube					

Responding to incidents of misuse- Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police. Where a parent alleges an image of a pupil at Shottery St Andrew's CE Primary has posted or been the victim of a posting of an inappropriate image, members of staff should NOT attempt to verify or view the image . The DSL must be immediately informed.



How will e-safety complaints be handled?

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Website. Complaints of Internet misuse by pupils will be dealt with by the class teacher and recorded on the appropriate form. Any incidents of cyber bullying must be reported to the Headteacher. Any complaint about staff misuse must be referred to the Head teacher who should use the agreed WCC procedures. Pupils and parents will be informed of the complaints procedure through the reading of this policy.

School / Academy Actions & Sanctions

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. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Actions and Sanctions - Pupils								
Incidents	Refer to class teacher	Refer to Headteacher	Refer to ICTDS for action	Inform parents/ carers	Removal of network/ internet access rights	Warning	Further sanction eg exclusion	Refer to Police
Deliberately accessing or trying to access material that could be considered illegal, unsuitable or inappropriate.								
Unauthorised use of non-educational sites during lessons								
Unauthorised use of mobile phone / digital camera / other mobile device								
Unauthorised use of social media/ messaging apps / personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school / academy network by sharing username and passwords								
Attempting to access or accessing the school / academy network, using another student's / pupil's account								
Attempting to access or accessing the school / academy network, using the account of a member of staff								
Corrupting or destroying the data of other users								
Sending an email, text or 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 / academy'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								

Actions Sanctions - Staff

Incidents	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to ICTDS	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).							
Inappropriate personal use of the internet / social media / 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 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 students / pupils							
Actions which could compromise the staff member's professional standing							
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy							
Using proxy sites or other means to subvert the school's / academy'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							

Appendix 1 –E -Safety Contacts and References

Warwickshire ICT Development Service Desk 01926 414100

Safety in Schools and Schools e-Safety Policy: http://www.clusterweb.org.uk?esafety

WMNet e-Safety Pledge: http://www.wmnet.org.uk/esafetypledge/

Schools e-Safety Blog: http://www.clusterweb.org.uk?esafetyblog

Child Exploitation & Online Protection Centre: http://www.ceop.gov.uk/contact_us.html

Virtual Global Taskforce – Report Abuse: http://www.virtualglobaltaskforce.com/

Think U Know website: http://www.thinkuknow.co.uk/

Becta: http://www.becta.org.uk/schools/safety

Internet Watch Foundation: http://www.iwf.org.uk/

Internet Safety Zone: http://www.internetsafetyzone.org.uk/

KidSMART: http://www.kidsmart.org.uk/

NSPCC: http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Childline: http://www.childline.org.uk/

NCH – The Children's Charity: http://www.nch.org.uk/stories/index.php?i=324

NCH – Digital Manifesto: http://www.actionforchildren.org.uk/uploads/media/29/5706.pdf

CBBC Safe Surfing including the Chat Guide: http://www.bbc.co.uk/cbbc/help/safesurfing/

Parents' Centre : http://www.parentscentre.gov.uk/usingcomputersandtheInternet/

Appendix 2

Legal framework

An awareness of legal issues is important, but this page is not definitive advice. Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly.

Possible offences:

Sexual Offences Act 2003

Grooming – If you are over 18 and have communicated with a child under 16 at least twice (including by phone or 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.

Making indecent images – it is an offence to take, make, distribute, show, advertise indecent images of a child under 18. (NB to view an indecent image on your computer means that you have made a digital image.)

Causing a child under 16 to watch a Sexual Act – to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.

Abuse of positions of trust - Staff must be aware that it is 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. (Applies to teachers, social workers, health professionals, connexions staff)

Information about the 2003 Sexual Offences Act can be found at www.teachernet.gov.uk

Relevant Legislation

The Computer Misuse Act 1990 - makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Public Order Act 1986 – offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

Communications Act 2003 - There are 2 separate offences under this act:

Sending by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.

Sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.

This wording is important because the offence under a. is complete when the message has been sent - no need to prove any intent or purpose. It is an offence under b. to keep using the network for sending any kind of message irrespective of content if for the purpose of causing annoyance etc.

Malicious Communications Act 1988 – offence to send a letter, electronic communication or article which is indecent or grossly offensive, threatening or false information with intent to cause distress or anxiety to the recipient.

Copyright, Design and Patents Act 1988 - it is an offence to use unlicensed software

Protection of Children Act 1978 - The law on images of child abuse is clear. It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom.

Obscene Publications Act 1959 and 1964 - defines “obscene” and related offences.

Protection from Harassment Act 1997

Section 2 - 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.

Section 4 - 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.