SNITTERFIELD PRIMARY SCHOOL

E-Safety

POLICY

This version	July 2016
Adopted by the Governing Body	13th July 2016
Review date	July 2017

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
The school's e-safety policy operates in conjunction with other policies including: Student Behaviour, Bullying, Curriculum, Data Protection and Security.

This policy has been adapted from the Warwickshire ICT development service's core E-safety policy which was strongly influenced by the work of the Kent E-safety team and based on advice given by the Metropolitan police.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- *Responsible ICT use by schools including all staff and pupils, as well as parents, governors and advisers; encouraged by education and made explicit through published policies.*

- *Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.*

- *Safe and secure broadband from the Warwickshire Broadband including the effective management of Websense filtering and Policy Central monitoring.*

- *National Education Network standards and specifications.*

Further Information

Warwickshire ICT Development Service   01926 414100
Emma Arkill, e-Learning Adviser   emmaarkill@warwickshire.gov.uk
Jane Key, Senior e-Learning Adviser   janekey@warwickshire.gov.uk

E-Safety Audit

This quick audit will help the senior management team (SLT) assess whether the basics of E-Safety are in place to support a range of activities that might include those detailed within Appendix 1.

The school has an e-Safety Policy that complies with ICTDS guidance.	Y
Date of latest update: **July 2016**	
<mark>The Policy was agreed by governors on:</mark>	
The Policy is available for staff in: **Policy file, ICT Co-ordinators file and on the school website**	
And for parents in: **School office and on the school website**	
The Designated Child Protection Coordinator is: **Monica Gamble**	
The e-Safety Coordinator is: **Amanda Norris**	
How is e-Safety training provided? **External training is fed back to staff, via MG or AN.** **Cross federation training will also take place.**	
Is the Think U Know training being considered?	Y
All staff are encouraged to sign an Acceptable ICT Use Agreement on appointment.	Y
Parents read and acknowledge an agreement that their child will comply with the school Acceptable ICT Use policy.	Y
Rules for Responsible Use have been set for pupils:	Y
These Rules are displayed in all rooms with computers.	Y
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	Y
The school filtering policy has been approved by SLT.	Provided by LA
School personal data is collected, stored and used according to the principles of the Data Protection Act.	Y
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SMT.	Y

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for Computing and for Child Protection.

- *The schools e-safety Co-ordinator is **Amanda Norris**.*

- *Our e-Safety Policy has been written by the school, building on the Warwickshire ICT Development Service e-Safety Policy and government guidance. It has been agreed by the Executive Head Teacher, senior management and approved by the governors.*

- *The e-Safety Policy will be reviewed annually.*

Teaching and learning

Why Internet use is important:

- *Internet use is part of the statutory curriculum and is a necessary tool for learning.*

- *The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.*

- *The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.*

- *Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security when using the internet.*

How does Internet use benefit education?

Benefits of using the Internet in education include:

- *Access to world-wide educational resources including museums and art galleries;*

- *Inclusion in the National Education Network which connects all UK schools;*

- *Educational and cultural exchanges between pupils world-wide;*

- *Vocational, social and leisure use in libraries, clubs and at home;*

- *Access to experts in many fields for pupils and staff;*

- *Professional development for staff through access to national developments, educational materials and effective curriculum practice;*

- *Collaboration across support services and professional associations;*

- *Improved access to technical support including remote management of networks and automatic system updates;*

- *Exchange of curriculum and administration data with the LA and DfE;*

- *Access to learning wherever and whenever convenient.*

Internet use will enhance learning

- *The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.*

- *Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.*

- *Internet access will be planned to enrich and extend learning activities.*

- *Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.*

- *Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.*

Pupils will be taught how to evaluate Internet content

- *If staff or pupils discover unsuitable sites, the URL (address), time, date and content is reported to Amanda Norris, who notifies Warwickshire ICT Development Service.*

- *The school will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.*

Managing Internet Access

Information system security

- *The security of the school information systems will be reviewed regularly by ICTDS through our subscription to the web server.*

- *Virus protection will be installed and updated regularly by ICTDS through our subscription to the web server.*

- *The school uses the Warwickshire Broadband with its firewall and filters.*

- *The school provides an addition level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Service.*

- *Portable media may not be taken out of school without specific permission.*

- *Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.*

- *Files held on the school's network will be regularly checked.*

- *Monica Gamble and Amanda Norris are the only members of staff who have access to Administrator codes relating to the school network and wireless.*

E-mail

- *Pupils may only use approved e-mail accounts on the school system. This will only take place in lessons where children are taught how to use e-mail, pupils will not access e-mails within school at any other time.*

- *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.*

- *Use of words included in the Policy Central 'banned' list will be detected by WCC Web Sense and logged.*

- *Access in school to external personal e-mail accounts may be blocked.*

- *Members of staff use a school e-mail address rather than a personal address when e-mails sent are related to school matters.*

- *E-mail sent to external organisations should be written carefully in the same way as a letter written on school headed paper.*

- *The forwarding of chain letters is not permitted.*

Published content and the school website

- *The contact details on the Website are the school address, e-mail and telephone number. Staff or pupils personal information will not be published.*

- *Email addresses will be published carefully, to avoid spam harvesting.*

- *_____ will take overall editorial responsibility and ensure that content is accurate and appropriate.*

- *The Website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.*

Publishing staff and pupil's images and work

- *Photographs that include pupils will be selected carefully.*

- *Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.*

- *Written permission from parents or carers will be obtained at the beginning of each school year, before photographs of pupils are published on the school Web site. Permission slips are located in the school office.*

- *Pupil's work will only be published with the permission of the pupil and parents.*

- *Images of staff will not be published without consent.*

Social networking and personal publishing

- *Social networking sites and newsgroups will be blocked.*

- *Pupils and staff 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.*

- *Pupils and parents will be advised that the use of social networking spaces outside school may be inappropriate for primary aged pupils.*

- *Pupils and staff are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.*

- *Teachers' official blogs or wikis should be password protected and run from the school website. Teachers are advised not to run social network spaces for pupils or to accept pupils or parents as friends on social networking sites.*

- *Pupils and staff are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. They are encouraged to invite known friends only and deny access to others. Guides for staff relating to use of Social Networking sites can be found in the Staffroom and in the ICT Co-ordinators file.*

- *Pupils and staff are advised not to publish specific and detailed private thoughts.*

- *The school is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.*

<u>Managing filtering</u>

- *The school works in partnership with the Warwickshire ICT Development Service and Becta to ensure filtering systems are as effective as possible.*

- *If staff or pupils discover unsuitable sites, the URL, time and date must be reported to Amanda Norris or Monica Gamble who will inform WCC.*

- *Monica Gamble and Amanda Norris will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.*

- *Any material that the school believes is illegal will be reported to appropriate agencies such as IWF or CEOP.*

Managing videoconferencing

<u>The equipment and network</u>

- *All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.*

- *IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.*

- *Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.*

- *External IP addresses should not be made available to other sites.*

- *Videoconferencing contact information will not be put on the school web site.*

- *School videoconferencing equipment will not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.*

<u>Users</u>

- *Pupils will not make or answer a videoconference call. This will only be carried out by a Teacher.*

- *Any lessons involving videoconferencing will be supervised by a Teacher at all times.*

- *Permission from parents will be sought if a lesson requires videoconferencing.*

- *Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.*

Content

- *When recording a lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.*

- *Recorded material shall be stored securely.*

- *If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).*

- *Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.*

Managing emerging technologies

- *Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. We take advice on new technologies from ICTDS.*

- *Mobile phones will not be used by pupils or staff during lessons or formal school time. Children are not to bring mobile phones into school. The sending of abusive or inappropriate text messages is forbidden.*

- *The school will regularly investigate cellular wireless, infra-red and Bluetooth communication. The only people who have access to the wireless password is Monica Gamble and Amanda Norris.*

- *Staff will only use a school phone where contact with parents is required.*

Protecting personal data

- *Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.*

- *Any records or documents containing personal details relating to pupils (e.g. school reports) will only be kept on a secure encrypted memory stick.*

Policy decisions

Authorising Internet access

- *The school will maintain a current record of all staff and pupils who are granted Internet access.*

- *All users must read, sign and abide by the 'Acceptable ICT Use Policy' before using any school ICT resource.*

- *Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.*

- *Parents are informed that pupils will be provided with supervised Internet access.*

- *Parents are asked to read and acknowledge the school's 'Acceptable ICT Use Policy'.*

Assessing risks

- *In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take 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 WCC can accept liability for the material accessed, or any consequences of Internet access.*

- *The Head Teacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.*

- *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.*

Handling e-safety complaints

- *Complaints of Internet misuse will be dealt with by a senior member of staff*

- *Any complaint about staff misuse must be referred to the Head Teacher who should use the agreed WCC procedures.*

- *Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.*

- *Pupils and parents will be informed of the complaints procedure.*

- *Parents and pupils will need to work in partnership with staff to resolve issues.*

- *Sanctions within the school discipline policy include:*

- *interview/counselling by _____;*
- *informing parents or carers;*
- *removal of Internet or computer access for a period.*

Community use of the Internet

- *The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking and gaming sites, and offer appropriate advice.*

Communications Policy

Introducing the e-safety policy to pupils

- *Rules for Internet access are posted in all networked rooms.*

- *Pupils are informed that Internet use will be monitored.*

- *Pupils will be introduced to and taught e-safety in Computing lessons to raise the awareness and importance of safe and responsible internet use both in school and at home.*

- *Instruction in responsible and safe use should precede Internet access.*

Staff and the e-Safety Policy

- *All staff are given the School e-Safety Policy and its importance explained.*

- *Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.*

- *All staff will read and sign the Warwickshire Acceptable ICT Use Policy.*

- *Staff development in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.*

Enlisting parents' support

- *Parents' attention is drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Website.*

- *Internet issues will be handled sensitively to inform parents without alarm.*

- *A partnership approach with parents is encouraged. This could include Parents' Workshops with demonstrations and suggestions for safe home Internet use.*

- *Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.*

Monitoring and Review

It is the responsibility of all staff to follow the principles stated in this policy.
This policy will be reviewed in July 2017 or as necessary.