Policy:	**E-safety Policy** September 2018	
Status:	Non Statutory	
Review Date:	3 yearly - September 2021	

General Policy Statement

St Botolph's C of E Primary School takes the safety of all children and adults very seriously and the policy is written to protect all children and adults. This E-Safety Policy recognises and seeks to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others. We recognise that E-Safety encompasses not only internet technologies, but also electronic communications such as mobile phones and wireless technology.

What does electronic communication include?

- Internet collaboration tools: websites, social networking sites and web-logs (blogs);
- Internet research: websites, search engines and web browsers;
- Mobile phones and Tablets / iPads;
- Internet communications: e-mail and IM;
- Webcams and video-conferencing;
- Wireless games consoles.

The risks

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school.

However, it is also important to consider the risks associated with the way these technologies can be used. These risks to e-safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Incidents will vary from the unconsidered action to considered illegal activity.

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

As a school it is our duty of care alongside that of parents and other members of the community to protect our children from these dangers and we are committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the risks that exist so that they can take an active part in safeguarding children. The purpose of this e-safety policy is to outline what measures the school takes to ensure that pupils can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion. We will use education, technology, accountability, responsibility and legislation as the key ways to achieve this. The school will review the policy regularly and revise the policy annually to ensure that it is current and considers any emerging technologies.

- The school will audit their filtering systems regularly using Lightspeed Systems to ensure that inappropriate websites are blocked.
- To ensure that pupils and staff are adhering to the policy, any incidents of possible misuse will need to be investigated.
- The school will include e-Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. pupils need to know how to control and minimise online risks and how to report a problem.
- All staff must read and sign the Acceptable Use Policy.
- Parents should sign the Acceptable Use Policy in their child's home-school diary.
- The e-Safety Policy will be made available to all staff, governors, parents and visitors through the school website.

Implementation and Compliance: No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences.

1. **Whole school responsibilities for e-safety**

Within the school all members of staff and pupils are responsible for e-safety. Responsibilities for each group include:

All Staff (including peripatetic, school governors and volunteers)

Staff are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported.

- Have a clear understanding of e-safety issues and the required actions from e-safety training sessions.
- Report any e-safety issues to the computing coordinator and headteacher, as soon as the issue is detected.
- Comply with a highly visible staff Acceptable Use Policy (AUP) which staff must sign each year and abide by each time they use school ICT equipment and systems, either in the school or elsewhere

Teaching Staff

- Educate pupils on e-safety through specific e-safety lessons and reinforcing this in the day to day use of ICT in the classroom.

Pupils

- Participate in and gaining an understanding of e-safety issues and the safe responses from e-safety lessons.
- Comply with a highly visible student's Acceptable Use Policy (AUP) which pupils must abide by each time they use school ICT equipment and systems either in the school or elsewhere.
- Report any e-safety issue to the teacher, support staff or parent.
- Take responsibility for their own actions using the internet and communications technologies.

Computing Coordinator, Headteacher and Shepshed High School Support Team

- Ensure that the best technological solutions are in place to ensure e-safety as well as possible, whilst still enabling pupils to use the internet effectively in their learning.
- Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition securing and preserving evidence of any e-safety breach.
- Deal with e-safety breaches from reporting through to resolution in conjunction with the SLT team
- Work with SLT and governors to create, review and advise on e-safety and acceptable use policies.
- Work with outside agencies including the police where appropriate.
- Maintain a log of all e-safety issues.
- Monitor the technology systems which track student internet use to detect e-safety breaches.
- Assist in the resolution of e-safety issues with other members of staff

2. **Teaching and learning**

Why is internet use important?

St Botolph's C of E Primary School recognises the internet and other digital technologies provide a vast opportunity for children and adults to raise educational standards, stimulate awareness, enhance and enrich learning, support the professional work of staff and to enhance the school's management functions. Developing effective practice in internet use for teaching and learning is essential. The Internet use is part of the statutory curriculum and 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. pupils use the internet widely outside of school and will need to learn how to evaluate internet information and to take care of their own safety and security. The school internet access will be designed expressly for student 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. Access levels will be reviewed to reflect the curriculum requirements;
- Staff should guide pupils in on-line activities that will support the learning outcomes planned;
- 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 expected to exercise the values of St Botolph's C of E school when working on the internet.

Evaluating Internet Content

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.

- Users must act reasonably;
- Users must take responsibility for their network use. For all staff, flouting electronic use policy is regarded as a matter for discipline;
- Servers will be located securely and physical access restricted;
- The server operating system will be secured and kept up to date;
- Virus protection for the whole network will be installed and current;
- Access by wireless devices must be pro-actively managed.
- The security of the school information systems will be reviewed regularly;
- Personal data sent over the internet should be encrypted or otherwise secured;
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail;
- The support team will review system capacity regularly.

Emails

- Pupils may only use approved e-mail accounts;
- 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;

School Website

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupils' personal information must not be published.
- E-mail addresses should be published carefully, to avoid spam harvesting.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should respect intellectual property rights and copyright.

Use of Images

- Pupils' full names will not be used anywhere on the website or internet collaboration tools, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.

Social Networking

- The schools will block/filter access to social networking sites;
- Newsgroups will be blocked unless a specific use is approved;
- Pupils will be taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations:
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be 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 should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school;
- Teachers should be advised not to run social network spaces for student use on a personal basis.

Filtering

The school will work with Shepshed High School, Schools Broadband and Lightspeed to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to the computing coordinator or headteacher. This task requires both educational and technical experience. The support team from Shepshed High School will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Mobile phones will not be used during lessons or formal school time and will be kept in locations away from the classrooms. The sending of abusive or inappropriate text messages is forbidden.

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

Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications;
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource;
- At Key Stage 2, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials;
- Parents will be asked to sign and return a consent form for student access.

Internet Risks

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. Neither the school nor Leicestershire CC can accept liability for the material accessed, or any consequences resulting from internet use. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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.

E-Safety Complaints

- Complaints of internet misuse will be dealt with by the headteacher;
- All pupils will be taught to use the internet safely and about the role of CEOP to monitor and report abuse;
- Any complaint about staff misuse must be referred to the headteacher, unless it is the headteacher where complaints will be sent to the Chair of Governors;
- Parents and pupils will be informed of the complaints procedure;
- Parents and pupils will need to work in partnership with staff to resolve issues.

Introducing the Policy

- Safety training will be given to all to raise the awareness and importance of safe and responsible internet use;
- Instruction in responsible and safe use should precede internet access;
- All staff will be given the School e-Safety Policy and its application and importance explained;
- Staff should be aware that internet traffic can be monitored;
- Discretion and professional conduct is essential;
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues;
- Parents' attention will be drawn to the school's e-Safety Policy in newsletters and through the website;
- Internet issues will be handled sensitively, and parents will be advised accordingly.

Websites offering additional advice and guidance

BBC Chat Guide
http://www.bbc.co.uk/chatguide/

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

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

Grid Club and the Cyber Café
http://www.gridclub.com

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

Internet Safety Zone
http://www.internetsafetyzone.com/

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

NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209

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

Stop Text Bully
www.stoptextbully.com

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

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

Appendix

The purpose of this e-safety appendix is to outline what measures the school takes to ensure that pupils can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

The following are provided for the purpose of example only. Whenever a pupil or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the headteacher.

Pupils:

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in school e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: referred to teacher; contact with parent; removal of internet access rights]

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to headteacher; contact with parent; removal of internet access rights for an extended period; exclusion]

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet

[Possible Sanctions: referred to headteacher; contact with parents; removal of equipment; removal of Internet access rights for an extended period; exclusion; referral to police]

Category D infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to headteacher; exclusion; removal of equipment; referral to police; LA e-safety officer]

Staff:

Category A (Misconduct)

- *Excessive* use of internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

[Sanction - referred to headteacher; Warning given.]

Category B (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the School into disrepute.

[Sanction – Referred to headteacher and potential school disciplinary procedures; Referred to police; Referred to governors]

Child Pornography:

In the case of child pornography being found, the member of staff will be immediately suspended and the school disciplinary procedures implemented.

Other safeguarding actions:

- Remove the computer to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.
- Where appropriate, involve external agencies as part of these investigations.