St Swithun's C of E School Online Safety Policy

January 2016

Introduction

St Swithun's C of E School takes the safety of all children and adults very seriously. This policy is written to protect all children and adults. We recognise that online Safety encompasses not only internet technologies, but also electronic communications such as mobile phones and wireless technology.

What does electronic communication include?

- Internet research: websites, search engines and web browsers;
- Internet communications
- Webcams
- Wireless games consoles.
- Mobile phones

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.

This online Safety Policy should recognise and seek 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. It should also give a framework for how potential online safety issues are to be dealt with should they be encountered.

What are the risks of using the internet?

- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats;
- Identity theft
- Publishing inappropriate content;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;

Roles and Responsibilities

- The school's Computing Co-ordinator will act as the online safety Co-ordinator, and will work closely with the Safeguarding Officer(s) to ensure matters that arise regarding safeguarding and bullying are dealt with in line with the schools policies for these matters. The online safety Co-ordinator will keep a record of internet misuse in or out of school that are is not seen as immediate safeguarding concerns (As these issues will be recorded in accordance with the Safeguarding Policy). Those that are safeguarding issues will be directly reported to the Safeguarding Officer(s).

- The online safety coordinator should maintain the online Safety Policy, manage online safety training and keep abreast of local and national online safety awareness campaigns. The online safety co-ordinator will feedback relevant information to 'whole school safety' to the designated safeguarding officers in the school.

- 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 in accordance with the local authority guidelines to ensure that inappropriate websites are blocked.

- The school will include online safety in the Computing 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 children will be taught to use the internet safely and school 'Computing and online safety monitors' will promote the importance of online safety regularly during ICT sessions.

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. Anything that the staff are not sure about must be relayed to the online safety officer to ensure the children's protection when learning online.

Teaching and learning

Why is Internet use important?

Developing effective practice in Internet use for teaching and learning is essential. 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 functions. The internet use is part of the statutory curriculum and a necessary tool for learning. St-Swithun's school has a duty to provide students with quality Internet access as part of their learning experience. 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. 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. Access levels will be reviewed to reflect the curriculum requirements and age of pupils;

• 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.

Evaluating Internet Content

Pupils should be taught what to do if they experience material that they find inappropriate, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

Incidents of a child reporting something they find inappropriate will first of all be reported to their class teacher, and if deemed appropriate, the teacher will refer the matter the online safety co-ordinator to ensure the internet filters are fully protecting the children.

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

Local Area Network security

• Users must act reasonably;

• Users must take responsibility for their network use. For all staff, flouting the Code of Conduct policy outlines the expectations for staff regarding internet use and matters arising

• 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.

Network Security

All internet connections must to ensure compliance with the Local Authority security policy. Firewalls and switches are configured to prevent unauthorised access between schools.

• The security of the school information systems will be reviewed regularly; • Virus protection will be updated regularly;

• Security strategies will be discussed with the LA when necessary;

• Personal data sent over the Internet should be encrypted or otherwise secured;

• Portable media may not be used with the schools network 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; • The ICT co-ordinator / network manager will review system capacity regularly. Emails

Use of Images

Refer to the Home School agreement regarding the use of photos in school.

Social Networking

• Matters arsing regarding safeguarding on Social Media will be reported directly to the schools Safeguarding Officer and the safeguarding protocol will be followed.

- Matters arising regarding bullying on Social Media will be dealt with by the class teacher or senior leadership team in accordance with the anti-bullying policy.
- Social Media cannot be accessed in school via the network.

Mobile Phones

Currently Mobile Phones are not used by any pupils in school and therefore are not permitted on the premises. If, in extenuating circumstances, a mobile phone is required by a pupil, they must take full responsibility for it. It will be kept in the school office and the school is not liable for any damage caused to the phone whilst on the school premises.

Computing resources

• At Key Stage 1 access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials;

• At Key Stage 2, children will be allowed access to the internet to support their learning on a filtered network. Reminders regarding internet safety and how to deal with inappropriate content will occur regularly in lessons so the children are equipped to browse the internet safely in school and at home.

• 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 Oxfordshire Council can accept liability for the material accessed, or any consequences resulting from Internet use. The school will audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

• Any complaints regarding the missue of the internet or ICT by staff members will be dealt with in accordance with the complaints policy.

Introducing the Policy

• Pupils will be informed that network and Internet use will be monitored;

• Online Safety monitors will meet termly with the online safety monitor to 'top-up' understanding and awareness so that this can be delivered back to their peers.

• Instruction in responsible and safe use should precede Internet access;

• Online safety module will be included ICT curriculum in both KS1 and KS2.

• All staff will be given the School online safety Policy and its application and importance explained.

• Parents' attention will be drawn to the importance of online Safety when there is information relevant to the children's safety online.

- Internet issues will be handled sensitively, and parents will be advised accordingly.

Review of the Policy

The Policy will be formally reviewed each year to ensure it is still inline with current guidelines. As technology is continually progressing, immediate concerns we are not yet aware of will be annotated onto the policy, and the schools online safety leader will liase with the designated online safety governor to keep them up to date of the measures the school takes to ensure the safety of children online.

Signed:……..(Head teacher)

Signed:…….. (Governors)

Date for Review:…….