Barrowby Church of England Primary School

E-safety policy

1. Introduction

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, bullying and for child protection.

1.1 The head teacher will act as an e-Safety Coordinator in relation to her role with child protection. It is not a technical role. The Computing subject leader and technician will support this role with regular monitoring and updating of firewalls and virus protection.

1.2 Our e-Safety Policy has been written by the school, building on the government guidance. It has been agreed by senior management and approved by governors.

2. Teaching and learning

2.1 Why the Internet and digital communications are important

- 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.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2. 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. For children below Year 5 Kidrex will be set as the default web-browser and Google for Years 5 and 6.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet, mobile technology and digital technology use.

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

- Pupils will be shown how to publish and present information to a wider audience.

2.3 Pupils will be taught how to evaluate Internet content

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

- Pupils will be taught the importance of cross-checking information before accepting its accuracy.

2.4 Managing Internet Access

2.4.1 Information system security

- School IT systems security will be reviewed regularly.

- Virus protection will be updated regularly.

- Security strategies will be discussed with the Local Authority and InfoTech Direct.

2.4.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.

- Pupils must immediately tell a teacher if they receive offensive e-mail.

- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- The school will carefully monitor how e-mail from pupils to external bodies is presented and controlled.

- The forwarding of chain letters is not permitted.

2.5 Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.

- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.6 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that their image cannot be misused. Pupils photographs will **only** be used if parental consent has been given.

- Pupils full names will not be used anywhere on the school Web site in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

- Work can only be published with the permission of the pupil and parents / carers.

- .Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.7 Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.

- Social networking sites such as Facebook; Whatsapp; MSN and Twitter are permanently blocked by our school servers. Pupils and staff cannot log onto or search these sites in the school environment.

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location and will be taught about the dangers of doing so.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

- Pupils will be advised to use nicknames and avatars **if** using social networking sites outside of school and when using the school blog.

2.8 Managing filtering

- The school will work with the local authority, Infotech and Becta to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to an adult in school who will report this to the e-Safety Coordinator.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.9 Managing videoconferencing & webcam use

- Videoconferencing and the use of webcams should use the educational broadband network to ensure quality of service and security.

- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

- Videoconferencing and webcam use will be appropriately supervised by school staff.

2.10 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.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

- Staff will not be allowed to use their phones as a method for photography.

- Games machines including Playstations, xboxes and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

- Staff will be issued with a school camera to capture photographs of pupils.

- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

2.11 Protecting personal data

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

2.12 Policy Decisions

2.12.1 Authorising Internet access

- All staff must read and sign the “Staff Code of Conduct for IT” before using any school IT resource.

- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.

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

- Any person not directly employed by the school will be asked to sign an "acceptable use of school IT resources" before being allowed to access the internet from the school site.

2.13 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Lincolnshire County Council can accept liability for any material accessed, or any consequences of Internet access.

- The school should audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

2.14 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 headteacher.

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

2.15 Communications Policy
2.15.1 Introducing the e-safety policy to pupils

- e-Safety rules will be posted in school and discussed with pupils regularly.

- Pupils (where appropriate) will be informed that network and Internet use will be monitored and appropriately followed up.

2.16 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.

- Staff from InfoTech that manage filtering systems or monitor IT use will be supervised by senior management and work to clear procedures for reporting issues.

- Staff will always use a child friendly safe search engine when accessing the web with pupils.

2.16 Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

- The school will maintain a list of e-safety resources for parents / carers.

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Updated April 2015.