Fishergate Primary E-Safety Policy

ICT (Information communication Technology) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. There is a need to build in the use of these technologies into our curriculum in order to arm our young people with the skills to access life-long learning and employment.

E-Safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Fishergate Primary. The term 'E-Safety' is used to encompass the safe use of all online technologies in order to safeguard children and adults from known and potential risks.

What does electronic communication include?
- Internet collaboration tools: social networking sites and web-logs (blogs);
- Internet research: websites, search engines and web browsers;
- Mobile phones
- Internet communications: e-mail and IM (Instant Messenger)
- Webcams and videoconferencing
- Wireless games consoles

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 will be dealt with quickly and within line with this policy. Teachers 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 immediately. Fishergate Primary will 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.

What are the risks?
- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats;
- Identity theft;
- Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data.

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 shall be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure. Discussions will be held with the Local Authority Designated Officer for safeguarding and/or a community police officer to establish procedures for handling potentially illegal issues.

This policy aims to inform how pupils and parents/carers are part of the procedures and how children should be educated to make good judgements about what they see, find and use.

Fishergate Primary E-Safety Policy

<u>Implementation and Compliance</u>
No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences. In line with the Children's Act 2004 and the government's guidance document 'Working Together to Safeguard Children', it is the responsibility of schools to ensure that children and young people are protected from potential harm both within the school environment and beyond. It is therefore essential that there is active involvement of both children and their parents/carers for the successful use of online technologies.

<u>Teaching and learning:</u>

<u>Why is Internet use important?</u>
The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

The school Internet access is designed expressly for pupil use including appropriate content filtering.
Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
As part of the new ICT (computing) curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.
The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society.

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information

- 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.

<u>Evaluating Internet Content</u>
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. It is a sad fact that 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.

<u>Roles</u>

<u>Roles: School Leadership</u>
It is the role of the Headteacher and governors to:
- Ensure there is appropriate and up-to-date anti-virus and anti-spyware software on all susceptible devices and that this is reviewed and updated on a regular basis.
- Ensure that filtering is set to the correct level for staff and children.
- Provide up-to-date information for all staff to deliver e-safety effectively to pupils.
- Include parents/carers so they feel up-to-date with current government guidance and know where to go for advice.
- Ensure that all adults are aware of the schools filtering levels and why they are in place.
- Record any e-safety incidents to help inform future development and safeguarding.
- Ensure that the e-Safety policy is reviewed annually.

Fishergate Primary E-Safety Policy

Roles: Staff or adults at Fishergate Primary
It is the responsibility of all staff/adults within the School to:
- Ensure that they know who the Designated Person for Child Protection so that any incidents which involve a child can be reported quickly. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via digital technologies to the Designated Person for Child Protection.
- Be up-to-date with e-Safety information and education that is appropriate for the year group they work with and implant this through their teaching.
- Ensure that all children are protected and supported in their use of online technologies so that they know how to use them in a safe and responsible manner.
- Ensure that children know what to do in the event of an incident and who to talk to.
- Not disclose security passwords to others.
- Ensure USB drives are encrypted; if any data is required to be taken from the school premises.
- Report any accidental 'misuse' or access to inappropriate materials to the Designated Person for Child Protection
- Not use personal equipment such as mobile phones and digital cameras in school for work purposes. Any such use should be agreed or reported promptly to the Headteacher.
- Not to store any school personal data such as, pupil levels, pupil photographs or planning with names on it, at home.
- Keep the Headteacher up to date with any new issues, procedures and risks that may need to be included within this policy.
- Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff and adults

Roles: Children
Children will be:
- Expected to follow the Acceptable Usage Agreement whilst at school.
- Taught the importance of adopting good e-Safety practice when using digital technologies out of school.
- Taught the need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Roles: Parents/Carers
At Fishergate Primary School, we encourage our parents/carers to support the acceptable usage of the internet, within school and also at home. We hope that parents/carers will work together with pupils to develop their understanding of the importance of e-safety.

E-mail
- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:
- Pupils may only use approved internal e-mail software on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- E-mail sent to external organisations should be written carefully and authorised by the class teacher before sending from the teachers email account.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Fishergate Primary E-Safety Policy

Social Networking

- Social networking Internet sites (such as, Twitter, Facebook and Instagram) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others (if allowed home access)
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- The sending of abusive or inappropriate text messages is forbidden.
- On trips staff mobiles are used for emergency only
- Staff should always use the school phone to contact parents, unless in an emergency on a school trip.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom.
- Parents cannot use mobile phones on school trips to take pictures of the children.

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out by Fishergate School.
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.
- The Headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.
- Staff should always use a school camera to capture images and should not use their personal devices.
- Photos taken by the school are subject to the Data Protection Act.

Fishergate Primary E-Safety Policy

<u>Published Content and the School Website</u>

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act
- Staff and pupils' personal information will not be published.
- Photographs and videos that include pupils will be selected carefully.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Website.
- Parents should only upload pictures of their own child/children onto social networking sites.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Further Resources

We have found these web sites useful for e-safety advice and information.

http://www.thinkuknow.co.uk/	Set up by the Police with lots of information for parents and staff including a place to report abuse.
http://www.childnet-int.org/	Non-profit organisation working with others to "help make the Internet a great and safe place for children".

Policy prepared by: Mrs Sahar Dibden