Online safety Policy

Evidence of intentions and practice - for the information of staff, governors, parents, LA, OFSTED and DfE

Prepared by:
Mrs C Openshaw
Online Safety coordinator

Approved by:
Curriculum Committee

Issue date:

Review date:

PARKSTONE PRIMARY SCHOOL

Online Safety Policy

1. Writing and reviewing the Online Safety policy

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

- Mrs Openshaw (Online Safety Coordinator) works jointly with the Child Protection Officer (Mrs M Gill) as there is an overlap of the roles.
- Our Online Safety Policy has been written by the school, building on the Kent Online Safety Policy and 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 includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives and guidance for Internet use.
- 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 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.
- Pupils will be taught how to report unpleasant Internet content.

3. Managing Internet Access

3.1 Information system security

- School computing systems securities are reviewed regularly.
- Virus protection is updated regularly.
- Security strategies are all provided by the Local Authority.

3.2 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 should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

3.3 Published content and the school web site

- Staff or pupil personal contact information will not generally 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.

3.4 Publishing pupils' images and work

- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

3.5 Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Ideally pupils would use only moderated social networking sites such as the facility on the 'It's Learning' site, J2E and Edmodo (blogging).
- 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 and parents are advised that social network spaces such as Instagram, Twitter and Facebook have a minimum age requirement of 13 for setting up an account.
- Pupils will be advised to use nicknames and avatars when using social networking sites, if they do have parental consent.

3.6 Managing filtering

- The school will use the Hull LA internet service provider 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 the Online Safety coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7 Managing videoconferencing and webcam use

- Videoconferencing 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 for the pupil's age.

3.8 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.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- 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.
- The use by pupils of cameras in mobile phones will be kept under review.
- Games machines including the Sony Playstation, Microsoft Xbox, Nintendo Wii 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 phone where contact with pupils is required.
- Staff will be issued with a class camera or iPad to photograph children.
- When staff are off site on school activities arrangements may be made to upload photographs to the school twitter account from mobile phones. This will be with permission from the Head. On return to school all photographs will be transferred immediately to the school server for storage and deleted from mobile phones.
- The appropriate use of Learning Platforms will be discussed within the school.

3.9 Protecting personal data

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

3.10 Facebook

All staff have access to a copy of the HGFL Handbook- 'Using Facebook Safely'. They are required to sign an agreement stating that they are fully aware of these guidelines. These guidelines include information about how to make your profile private and advise against befriending parents or pupils. If staff have any queries they should see Mrs Openshaw - Online Safety coordinator.

4. Policy Decisions

4.1 Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for Computing' before using any school computing resource.
- The school will maintain a current record of all staff and pupils who are granted access to school computing systems.
- Access to the internet will be adult led with directly supervised access to, approved on-line materials and monitored closely.
- Children are not allowed unsupervised access to the ICT suite or laptops at any time.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school computing resources' before being allowed to access the internet from the school site.

4.2 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. The school cannot accept liability for any material accessed, or any consequences of internet access.
- 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 and effective.

4.3 Handling Online 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.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the internet.

5 Communications Policy

5.1 Introducing the Online Safety policy to pupils

- Online Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and internet use will be monitored and appropriately followed up.
- A programme of training in Online Safety will be developed, possibly based on the materials from the Kent website.
- Online Safety training will be embedded within the Computing scheme of work or the Personal Social and Health Education (PSHE) curriculum.

- The whole school will take part in an annual Online Safety day. This will support the continuous provision for Online Safety within normal computing lessons.

5.2 Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff must be informed that network and internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT 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.

5.3 Staff and mobile phones, tablet devices and cameras

- Mobile phones owned by members of staff must not be kept on their person during times when they are in contact with pupils.
- Mobile phones should be left securely locked in staff safes, situated in the classroom. Mobile phones may be accessed before children enter the setting, during lunchtime and when all children have left at the end of the day.
- All students must leave mobile phones in the safe provided by the school administration staff.
- Any adult who operates as a volunteer within the setting must also adhere to the above procedure. Where possible a safe will be available which must be locked. If this is not possible the school administration officer will arrange for the mobile phone to be kept securely within her own safe.
- The use of tablet devices by staff is permitted where appropriate during lesson times (such as clarification of a word in a guided reading session).
- During times when tablets are not being used, they should be kept locked securely in a staff safe located in a classroom.
- The use of cameras within the setting is only permitted when it constitutes the collection of photographic evidence to support assessment. Each member of staff has a school camera or school iPad for this purpose. The downloading and development of photos must be done on site.
- Under no circumstances should a personal camera (or a tablet used for photography) be brought into the setting unless it has been confirmed and agreed to by the Headteacher.

5.4 Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School Online Safety Policy in newsletters, leaflets, through parent meetings, the school brochure and on the school website.
- The school will maintain a list of Online 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.

The policy will be reviewed annually.

Appendix 1: Useful resources for teachers

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/
Becta
http://schools.becta.org.uk/index.php?section=is
Chat Danger
www.chatdanger.com/
Child Exploitation and Online Protection Centre
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen
www.digizen.org/
Kent Online Safety Policy and Guidance, Posters etc
www.clusterweb.org.uk/kcn/Online Safety_home.cfm
Kidsmart
www.kidsmart.org.uk/
Kent Police – Online Safety
www.kent.police.uk/Advice/Internet%20Safety/Online Safety%20for%20teacher.html
Think U Know
www.thinkuknow.co.uk/
Safer Children in the Digital World www.dfes.gov.uk/byronreview/

Appendix 2: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Childnet International "Know It All" CD
http://publications.teachernet.gov.uk
Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Kent leaflet for parents: Children, ICT & Online Safety
www.kented.org.uk/ngfl/ict/safety.htm
Parents Centre
www.parentscentre.gov.uk
Internet Safety Zone
www.internetsafetyzone.com

School website

http://www.parkstone.hull.sch.uk