Pikes Lane Primary School
E- Safety
Statement of Practice

Subject Leader: Mr Bradley
Governing Body: Management Committee,
Last Updated: September 2017
Review Date: September 2018

E-Safety Statement of Practice

1.0 Introduction

The e-Safety Policy covers the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity. The policy highlights the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It also provides safeguards and rules to guide staff, pupils and visitors in their online experiences.

1.1 Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible IT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband from Light Speed Systems and Computeam.
- A global proxy pac operating on all devices that pupils take off site.
- A school network that complies with the National Education Network standards and specifications.

2.0 Writing and reviewing the e-safety policy

The e-safety policy operates in conjunction with others, including policies for Pupil Behaviour, Bullying, Curriculum, Data Protection, Child Protection and Security plus the Home-School Agreement.

The school have appointed an E-safety Governors commitee and an E-safety Point of contact (Computeam or via Mr Bradley) within school (Headteacher – Child Protection Lead).

Our e-Safety Policy has been written by the school, building on the Bolton e-Safety Policy and government guidance. It will be annually reviewed alongside other policies and submitted to governors and approved by leadership.

3.0 Teaching and Learning

3.1 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.

It should be noted that the use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

3.2 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 including for devices that are taken home. (1 to 1 iPad Programme).

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives 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.

3.3 Pupils will be taught how to evaluate Internet content

The school will ensure that information is made available related to the use of internet derived materials by staff and pupils to ensure it complies with copyright laws.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

0 Managing Internet Access

4.1 Information system security

Internet accesses, management and infrastructure is outsourced to specialists (currently computeam) as part of a service level agreement. Internet filtering and security is currently run and delivered through a subscription to lightspeed systems. The most recent upgrade was completed in Summer 2017 to put the network onto longhorn, regular upgrades will be scheduled throughout the year in the half day computeam visits

More information on the technical specification of the filtering services is available here:

http://computeam.co.uk/productsandservices/specialist-education-ict-support.html

http://community.lightspeedsystems.com/longhorn/

School IT systems capacity and security will be reviewed and improved regularly. Virus protection will be updated regularly and any problems will be highlighted to the IT Co-ordinator as soon as possible.Security strategies will be reported to and discussed with Computeam if the need arises .

4.2 E-mail/Messaging

Since the introduction of a mobile management system for iPads in December 2017
https://www.lightspeedsystems.com/en-uk/products/mobile-manager/
Email addresses are no longer needed for the distribution of apps and e-books. Previously these were created and administrated by school using Google-mail admin.

All Devices are now supervised and 'imaged' with a profile selected by the school which disables iMessage, does not allow the installation of messaging apps such as Whatsapp, Facebook Messenger etc, and prevents the creation of email addresses through the 'Mail' App,

Apple IDs are now created and managed in Apple School Manager.
https://www.apple.com/education/

Pupils may only use the messaging facilities that teachers can administrate, moderate and monitor (The School Blog comments, Showbie and iTunes U discussions). The School stores all messages and staff have admin rights to check and monitor these.

Pupils must immediately tell a teacher if they receive an offensive message.

Pupils must not reveal personal details about themselves or others in message communication, or arrange to meet anyone without specific permission. All communication should be approved by and shown to an adult.

E-mails written as part of a lesson (IE to send to an external organisation) should be written carefully and authorised by teacher before sending, in the same way as a letter written on school headed paper. This should not lead to pupils owning, creating or maintaining an email address that could be used by them in future for private communication.

All staff should treat incoming e-mail as suspicious and attachments not opened unless the author is known.

The forwarding of chain letters is not permitted.

Dialogue between pupils and teachers outside of the forums mentioned above is not allowed and any email correspondence between a teacher and parent should be forwarded and approved by a line manager or member of SLT.

Staff email addresses should only be used for school related correspondence and no discussion with colleagues or parents related to school matters should be entered into via a private email address.

Text messages to parents and pupils can only be sent via the school office and never from staff personal email.

This should be read in conjunction with the other policies mentioned in section 2.0

Staff and pupil email addresses created by school, managed apple ids and user accounts remain the property of the school and access for viewing and monitoring the related contents can be done with or without permission from the appropriate staff in necessary. Computeam remain the Super administrators for the email address access creation and monitoring.

4.3 Published content and the school Virtual Learning Environment and the school website

The Headteacher will delegate overall editorial responsibility to a member of staff to ensure that content is accurate, appropriate and quality of presentation is maintained.

4.4 Publishing pupil's images and work

Photographs that include pupils will be selected carefully through protection procedures (i.e. through a standard parental permission letter) and **will not** enable individual pupils to be clearly identified. Where possible group photographs will be used rather than full-face photos of individual children.

Pupils' full names will not be used on the Website (public area) or Blog, particularly in association with photographs.

Pictures of groups or group activities are preferred and consideration should be taken to ensure that identification is not clear to unknown persons.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website or blog.

Pupil's work can only be published with the permission of the pupil and parents.

Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
A list of pupils that cannot be photographed will be listed for staff and retained by the school. Pupils can not consent to photographs being taken if parents have objected. This should be read in conjunction to the other policies outlined in section 2.0.

4.5 Social networking and personal publishing

The school will block access to well known social networking sites on-site and via proxy and school will consider how to educate pupils in the dangers of using social media. Education in the safe use of social media does not suggest pupils should be allowed to access social media sites.

Newsgroups will be blocked unless a specific use is approved.

Pupils are advised never to give out personal details of any kind which may identify them or their location.

Pupils and parents are advised though the acceptable use of iPads policy that the only use of iPads should be for academic use. Social networking is not considered by school to fall within this category even if it is in some way related to school work.

Staff are given access to 'keeping your social media pages private' guidance and advised to regularly review their use of social networks to ensure boundaries between their personal life and professional role are clear. This includes:

- Checking the credentials of anybody asking to be your 'friend';
- Reviewing 'friend lists' regularly;
- Regularly checking the content profile;
- Avoid publishing material about your place of work;
- Use strong passwords for any social networking systems;

- Ensure your profile is set to ‘secure’ or ‘private’.
- Never add a Pikes Lane pupil to your friends list
- If you do receive a request from a pupil please inform the ICT Co-ordinator

- It is STRONGLY advised that sfaff do not add Pupils immediate family to social media sites even if they have a connection outside of school.

Any communication between staff and children should take place within clear and explicit professional boundaries. Staff should not share any personal information with the child or young person. They should not request, or respond to, any personal information from the child / young person, other than that which is appropriate as part of their professional role. Staff should ensure that all communications are transparent and open to scrutiny and in line with the teaching standards.

Up to date guidance for teachers can be found here
https://www.nasuwt.org.uk/article-listing/using-social-media-safely.html

More guidance for pupils and parents can be found here
http://www.childnet.com/resources/school-pack-for-online-safety-awareness

4.6 Managing filtering

The school will work closely with Computeam and Lightspeed Systems, who operate a comprehensive filtering system, which protects schools from accessing unsuitable material. It is constantly being updated to block access to new sites, which contain 'adult' texts or images. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a terminal. Neither the school, individuals nor Computeam LTD or Lightspeed Systems can accept liability for the material accessed, or the consequences thereof.

If pupils or staff, discover an unsuitable site, it must be reported to the Class Teacher, Safeguarding coordinator or Head teacher. Computeam will then be notified immediately with the exact address of the pages found so that they can be blocked quickly.

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

Lists of key words and site links connected to Radicalisation, Extremism and Terrorism are blocked for pupil access. Staff may have access only for educational purposes.

Weekly reports for searchers on the internet will be sent to the Extended Services Manager, IT Lead and Headteacher.

4.7 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 and games systems (e.g. Sony Playstations,

Microsoft Xbox) can bypass school filtering systems and present a new route to undesirable material and communications.

The use of portable media such as memory sticks and iPads will be monitored closely as potential sources of computer virus and inappropriate material. As new remote access technologies emerge, these will be explored by senior leaders. (See the data protsction policy.)

Pupils' mobile phones will not be permitted in school unless for emergency, in which case parents and teachers will have arranged for the device to be kept in the school office with no access during school hours.

The sending of abusive or inappropriate text messages is forbidden.

Staff will use a school phone where contact with pupils is required.

Staff should not use personal mobile phones during designated teaching sessions.

Staff can only use class digital cameras and iPad cameras. The use of personal cameras including mobile phones is forbidden,

4.8 Protecting personal data

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

5.0 Policy Decisions

5.1 Authorising Internet access

All staff must read and agree in writing to adhere to the Acceptable Use Policy for staff before using any school IT resource. A record of AUPs signed by all stakeholders will be kept within the Headteachers office.

Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Pupil eSafety Agreement to abide by the school's eSafety Rules. These eSafety Rules will also be displayed clearly in all networked rooms.

Pupils must also sign up to the Acceptable Use Policy (AUP) for Pupils. These will be stored in a central record of AUP's kept by the IT co-ordinator/ Extended services Lead.

Access to the Internet at Key Stage 1 will be by directly supervised access to specific, approved on-line materials.

At Key Stage 2 Internet access will be granted to a whole class as part of the scheme of work or to children who have asked the permission of an adult to use the Internet independently.
Teachers can make use of 'Apple Classroom' to guide pupils to resources and to track their actions.

Children at the upper end of the age range may be allowed to access the Internet independently, e.g. for private study or during wet play times.

All parents in Key stage 2 will be asked to sign the Acceptable use policy and agreement before taking iPads off the premise.

Any person not directly employed by the school will be asked to sign an Acceptable Use Policy before being allowed to access the internet from the school site.

It is a statutory requirement that pupils are taught to access the internet safely.

The statutory requirements for computing state:

Key Stage 1: use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the Internet or other online technologies.

Key Stage 2: select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

5.2 Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor Computeam can accept liability for the material accessed, or any consequences of Internet access.

The school will audit IT provision to establish if the eSafety Policy and all Acceptable Use Policies, are adequate and their implementation is effective. Govorners and SLT will take appropriate action if required which may mean recalling devices and short down time if unforeseen issues arise.

5.3 Handling eSafety 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).

5.4 Community use of the Internet

External organisations, or any persons not directly employed by the school, using the school's IT facilities must adhere to the eSafety Policy and the Acceptable Use Policy.

6.0 Communications Policy

6.1 Introducing the eSafety Policy to pupils

E-safety rules will be discussed with all pupils in computing lessons, whole school assemblies, class assemblies, circle times and PSHCE sessions.

Pupils will be informed that the blog, network and Internet use will be monitored and appropriately followed up.

A programme of training in e-Safety training is available for parents pupils and staff at
https://www.e-safetysupport.com/online_training

E-Safety training is embedded within the computing scheme of work and the Personal Social and Health Education (PSHE) curriculum.

The school participated in the safer internet day 2017
https://www.saferinternet.org.uk/safer-internet-day/2017
and will again in 2018
https://www.saferinternet.org.uk/safer-internet-day/2018

6.2 Staff and the eSafety Policy

The E-safety policy will be reviewed in September each year to meet the needs of the school. It will then be approved by governors and SLT in this time the previous policy will be in place.

All staff will be given the School e-Safety Policy via i-Books as soon as it is approved.

Any information downloaded must be respectful of copyright, property rights and privacy.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

A laptop or iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection, use of software and storage of the device. Staff can not allow anyone outside of school to use a school device (ie partner, friends or children).

6.3 Enlisting parents' support

Parents' attention will be drawn to the School eSafety Policy in newsletters, and the School Prospectus, and links on the school website or blog.

The app https://www.internetmatters.org/hub/esafety-news/new-e-safety-app-for-parents-and-children/
Will be put on all devices that will go home and more information will be included in the AUP.

7.0 Managing the Blog and iTunes U discussions

7.1 Access to the Blog

All staff will have a username and password to post on the Blog wich is hosted on the school website.
All children and the general public have access to post comments but these are moderated by staff before they are posted.
All passwords are stored in a secure area of the shared drive and are not accessible by pupils.

8.0 Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is issues are passed on the SLT / head of computing so that hey can be referred to the appropriate persons.

This policy is the Governors' responsibility and they review its effectiveness annually. They do this during reviews conducted between the, IT Co-ordinator, Designated Child Protection Coordinator, Governor with responsibility for IT and Governor with responsibility for Child Protection. Ongoing incidents would be reported to the full governing body.

The eSafety Policy was revised by Alex Bradley Head of computing in September 2017.

Date Approved TBC:

September 2017 Date for review: 2018 September

Appendix 1: Internet / Blog use - Possible teaching and learning activities

ctivities	ey eSafety issues
sing search engines to ccess information from range of websites.	upils should be supervised. upils should be taught what internet use is cceptable and what to do if they access material ney are uncomfortable with.
xchanging information ith other pupils and sking questions of xperts via e-mail.	upils should use only approved e-mail accounts. upils should never give out personal information. onsider using systems that provide online noderation e.g. Super Clubs.
ublishing pupils' work on chool and other ebsites.	upil and parental consent should be sought prior to ublication. upils' full names and other personal information nould be omitted.
ublishing images cluding photographs of upils.	arental consent for publication of photographs nould be sought. hotographs should not enable individual pupils to e identified. le names should not refer to the pupil by name.
udio and video onferencing to gather formation and share upils' work.	upils should be supervised. nly sites that are secure and need to be accessed sing an e-mail address or protected password nould be used.