Kennington Primary School

E-Safety Policy Policy

Reviewed by	Date	Signed
S. Pritchard	Feb 2016	S.Pritchard
S. Pritchard	Feb 2017	S. Pritchard

E-Safety Policy

The E-Safety Policy was created in conjunction with the following two documents:

The Lancashire e-Safety Framework Document
The Lancashire e-Safety Guidance Document

The Lancashire e-Safety Guidance Document offers support and prompts to enable schools to consider the appropriate responses to e-Safety in their settings and is intended to be used alongside the e-Safety Framework.

The e-Safety Framework Document enables schools to collate responses from the Guidance Document into the appropriate sections.

Contents

E-Safety Policy
Kennington Primary School

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our e-Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community is prepared to deal with the safety challenges that the use of technology brings. The policy is organised in in the following sections:

- Policies and Practices
- Infrastructure and Technology Education and Training
- Standards and Inspection.

2. School's vision for e-Safety

There is no getting away from that fact that technology is now part of our everyday lives. Whether it be at work, school or in the home the way we interact with technology and the way it interacts with us has changed rapidly over the last 20 years and will inevitably continue to do so. At Kennington Primary School, we have adopted many new technologies as we have seen the potential benefits they have in improving the outcomes for our children. We want to equip them with the basic skills needed for life in the 21st century. We understand that we have a responsibility to teach children about all aspects of technology including those ones which may make them vulnerable if used inappropriately. We also have a duty to our staff to provide them with a framework which allows them to remain safe whilst using new technologies with our young people.

3. The role of the school's e-Safety Champion

The e-Safety Champion in our school is our nominated person as a point of contact for e-Safety related issues and incidents. They will work closely with the Health and Safety Officer and ICT subject Leader to fulfil the role outlined below.

Our e-Safety Champion is Simon Pritchard

The role of the e-Safety Champion in our school includes:

- Responsibility for ensuring the development, maintenance and review of the school's e-Safety Policy and associated documents, including Acceptable Use Policies.
- Ensure that the policy is implemented and that compliance with the policy is actively monitored.
- Ensure all staff are aware of reporting procedures and requirements should an e-Safety incident occur.
- Ensure the e-Safety Incident Log is appropriately maintained and regularly reviewed.
- Personally keeping up-to-date with e-Safety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging e-Safety advice/training for staff, parents/carers and governors.
- Ensuring the SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with all the school's Designated Senior Person/ Child Protection Officer to ensure a coordinated approach across relevant safeguarding areas.

4. Policies and practices

This e-Safety policy should be read in conjunction with the following other related policies and documents:

- Child protection policy
- Anti-Bullying policy

- Health and Safety policy
- SEN policy

4.1 Security and data management

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than necessary
- Only transferred to others with adequate protection.

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

- Our school business manager and Head teacher map key information that is held.
- All staff are aware of the location of data and are aware of their legal responsibilities.
- Paper copies of data MUST be kept in a secure place where children or parents cannot access it easily. If removed from school premises it MUST be kept in a safe place and will be shredded once finished with.
- Any data that stored electronically MUST be saved on a device that has password protection or is encrypted and deleted once no longer needs to be used.

- Electronic data were possible should be worked on in school, but if needed at home it may be removed from school premises but only on devices that are password protected or encrypted.

- Where possible staff should use equipment provided by the school to work on data and NOT download onto personal devices.

- If data is e-mailed to a member of staff it MUST be sent to a school e-mail address and not a personal one.

- Staff MUST ensure that mobile devices that contain data are not left accessible to children (for example pen drives left in computers).

- If data is stolen or lost it MUST be reported to the head and police (for example if a car is stolen with a laptop in the boot) as soon as possible.

4.2 Use of mobile devices

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

- Staff or children will NOT connect mobile phones, games consoles or personal net books to the school network to prevent virus transfer.

- Any data storage devices MUST be virus checked before use on the school network system.

- Children are NOT allowed mobile phones on school premises. These will be taken from the child by the class teacher placed in a secure place and returned at the end of the day.

- Staff must NOT use personal devices such as smart phones to download e-mails from a school e-mail address that contains data.

4.3 Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

- Photographs and videos of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998) and we have written permission for their use from the individual and/or their parents or carers. Each parent gives consent electronically via the Parent Portal Any amendments can be made within the year by the parent or carer contacting the school office.

- Digital images MUST be stored on the school network, class section of the network, My Pictures. If on a teachers laptop it MUST be a school laptop and MUST be password protected. No digital images must be stored on personal devices for example mobile phones, cameras, laptops.

- Once children leave the school MOST photographs will be deleted the year after they have left. Some photos will be kept longer such as prospectus photos, special celebrations, class photos, whole school photos, special events (centenary) these will be kept as a historical record of these events.

- Staff and pupils are aware that full names and personal details will NOT be used on any digital media, particularly in association with photographs.

- Parents and carers that are invited to school events need to be made aware at the beginning of each event that the taking of photographs during the performance is permitted as long as they are for personal use. Where parents have breached these rules, parents will be asked to delete the images.

- All staff have been made aware of Social Networking Sites and been provided with Lancashire's advice on this. Staff MUST not use photographs taken on school premises on personal social networking sites.

- Staff MUST only use school equipment to take photographs of children and used for school purposes and photos should be deleted when no longer needed. Staff MUST NOT take photographs of children on their own personal equipment.

- Students or volunteers within school should check with the class teacher for which children parental consent has been granted for students/volunteers to take and use photographs. The photographs taken

- Will only be used as evidence of work undertaken within the school and where possible students and volunteers should avoid taking photographs of children.

- All members of staff taking photographs will ensure that the subject of the photograph is appropriately dressed and not participating in activities that could be misinterpreted.

4.4 Communication technologies

In our school we use a variety of communication technologies and need to be aware of the benefits and associated risks.

Email:

In our school the following statements reflect our practice in the use of email.

- Any member of staff wishing to use e-mail to contact outside agencies on school business MUST use a school e-mail address that is connected thorough the Lancashire Grid for Learning service. Staff MUST NOT use personal e-mail addresses to contact staff, governors, parents or pupils.

- E-mail address can be set up for any member of staff needing one by speaking to the Head, Bursar or Computing Co-ordinator.

- The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school e-mail accounts. Any incidents of SPAM should be reported to the Westfield Centre.

- All users are aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act.

- All users are aware that e-mail is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

- All users are aware that all e-mail communications may be monitored at any time in accordance with the Acceptable Use Policy.

- All users MUST immediately report any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social Networks:

Many adults and pupils regularly use Social Network sites, although the minimum age for registering for some of these excludes primary school pupils. These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

- If a social networking site is used by staff members, details must not be shared with pupils and privacy settings must be set at maximum and reviewed regularly.

- All staff MUST be aware that comments and photographs that are uploaded to Social Networking sites can be seen around the world and remain their forever.

- All staff using social networking sites MUST remember that content posted online should not:

    - not contravene confidentiality,

    - bring the school or staff into disrepute, -lead to valid parental complaints

    - be deemed derogatory towards the school and/or its employees -be deemed as derogatory towards pupils and/or parents and carers

    - Bring into question their appropriateness to work with children and young people. -not upload any photograph taken on school premises.

- Adults must not communicate with children using any digital technology where the content of the communication may be considered inappropriate or misinterpreted. Online communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should be discouraged.

- Pupils must NOT be added as 'friends' on any Social Networking site.

- Staff using social networking sites MUST read the guidance supplied by Lancashire County Council.

- If there are any incidents of cyber bullying by pupils who have left the school or parents this MUST be reported to the head so that it can be dealt with by Human Resources.

Mobile telephones:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:

- Staff will not use or have mobile phones switched on during class time. It is not acceptable to use personal mobile phones to support lessons. Any member of staff failing to follow this guideline will be dealt with under disciplinary action.

- Mobile phones MAY be used in school in your own time and when there are no children present.

- In the case of emergencies the school office MUST be contacted and staff should make other members of their family aware of this.

- Visitors to school, volunteers and students MUST be made aware of the use of mobile phones in school and our duty of care to our children.

- Staff on educational visits will provide as part of their risk assessment an emergency contact number, in the case of their own personal mobile phone this may be used for this purpose and for the duration of the visit only.

Web sites and other online publications

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

- Materials that are downloadable from the school website must be in a read only format (eg PDF) to prevent changes happening.

- Information on the school website is available for the whole world to see.

- Teaching staff members have access to edit their own year group gallery.

- The Head Teacher has overall responsibility of the editing of the website.

- The school website contains e-safety links for parents.

- All staff are aware of the guidance for the use of digital media on the website.

- All children as part of their curriculum incorporate e-safety and the dos and don'ts of using the internet.

Video conferencing:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

- Parental permission is sought at the beginning of each year for every child for participation in video and photographs. It is important to remember that even though the children are not appearing 'live' on the internet the images that are broadcast from school during a video conference could be captured as a snapshot or video clip from a system receiving the message. Children whose parents do not want them to participate in videos WILL be out of camera shot.

- When video conferencing make sure that cameras are placed carefully and don't over look sensitive areas such as changing rooms or toilet areas.

- Approval for the Head MUST be obtained in advance of a video conferencing session taking place. All session MUST be logged including date, time and name of the external organisation/person taking part.

- Pupils using video conferencing equipment MUST be supervised at all the times.

- All staff supervising video conferencing equipment should know the procedure to follow if they are unhappy with the content of a VC session e.g. how to 'stop' or 'hang up' the call.

- Copyright, privacy and Intellectual Property rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

Others:

We will update our policy as we introduce new technologies. We will consider what we feel to be acceptable and unacceptable use of these new technologies and risk assess them as we introduce them.

4.5 Acceptable Use Policy (AUP)

An Acceptable Use Policy is intended to ensure that all users of technology within school will be responsible and stay safe. It should ensure that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

AUP's are recommended for all Staff, Pupils and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed (see appendices 1, 2 and 3). We consider these as partnerships between parents/carers, pupils and the school to ensure users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology must be kept in school and be made available to all staff.

As a school we feel it is important that we provide our parents/carers with regular e-safety updates and awareness meeting.

4.6 Dealing with incidents

An 'Initial Cause for Concern' sheet will be completed and handed to the e-safety champion/DSL to record and monitor offences. These are located on the staffroom Safeguarding Board and in each classroom. These will be audited on a regular basis by the e-safety champion and ICT subject leader.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, eg police, CEOP, Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident (see appendix 5). Always report illegal content to the International Watch Foundation (http://www.iwf.org.uk). They are licensed to investigate – schools are not.

Examples of illegal offences are:

- Accessing child sexual abuse images

- Accessing non-photographic child sexual abuse images

- Accessing criminally obscene adult content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website.

Inappropriate use

It is more likely that our school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offences see table below.

Incident	Procedure/Sanctions
Accidental access to inappropriate materials.	• Close the laptop lid/Navigate to the home screen on the iPad • Child to tell a trusted adult • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Inform parents • Persistent 'accidental' offenders may need further disciplinary action.
Using other people's login and passwords maliciously.	• Inform designated e-safety champion • Enter details into incident log • Additional awareness raising of e-safety issues and AUP with individual child/classes • Inform parents • More serious or persistent offences may result in further disciplinary action in line with the behaviour policy.
Deliberate searching for inappropriate materials.	• Inform designated e-safety champion • Enter details into incident log • Additional awareness raising of e-safety issues and AUP with individual child/classes • Inform parents • More serious or persistent offences may result in further disciplinary

	action in line with the behaviour policy.
Bringing inappropriate electronic files from home.	• Inform designated e-safety champion • Enter details into incident log • Additional awareness raising of e-safety issues and AUP with individual child/classes • Inform parents • More serious or persistent offences may result in further disciplinary action in line with the behaviour policy.

- The e-safety champion is responsible for dealing with e-safety incidents.

- All staff are aware of different types of e-safety incidents and how to respond appropriately.

- Children are informed of procedures through the Digital Literacy, E-safety and Citizenship curriculum.

- Incidents will be monitor by the e-safety champion and the ICT subject leader on a regular basis.

- Framework for responding to incidents will follow e-safety incident/escalation procedures (see appendix 5)

5. Infrastructure and technology

Our school will ensure that our infrastructure /network is as safe and secure as possible. Our school subscribes to the Lancashire Broadband Service (one connect); internet content filtering service is provided by default (Lightspeed). It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included on the school's subscription and this has been installed on all computers and laptops in school and configured to receive regular updates.

Pupil Access:

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

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

Passwords:

- All staff are aware of the guidelines in the Lancashire ICT security framework for schools.
- All staff have a user name and password to access the school network
- All classes have a user name and password to access the school network
- The administrator user name and password for the school network is known by the school business manager, the head teacher and the Computing subject leader.
- Children though their leaning about e-safety are reminded of the importance of keeping passwords secure.
- All teacher laptops are password secured.

Software/hardware:

- All software bought by curriculum leaders is purchased with site licences to ensure that it can be installed on the school network.
- A record of up to date licences for software is maintained by the Computing subject leader.
- The Computing subject leader controls what software is installed onto the school system.

Managing the network and technical support:

- The servers, wireless system and cabling is located is a secure place were physical access is restricted.
- All wireless devices have had their security enabled.

- The wireless system is only accessible through a secure password.

- The ICT subject leader and technical support are responsible for managing the security of the school network.
- The safety and security of the network is reviewed on a regular basis

- All computers are regularly updated with critical software updates and patches

- All users have clearly defined access rights to our school network with use of usernames and in some cases passwords. Permissions are assigned by the Computing subject leader.

- No users other than the administrator are allowed to download executable file or install software.

- Users report any evidence of a breach of security too the Computing subject leader.

- We are able to use pen drives that have been encrypted to store data on and will follow guidelines outlined in section 4.

- Where a teacher is provided with a school laptop this MUST be used solely for school business and not personal use.

- The Computing subject leader and e-safety champion is responsible for liaising with and managing the technical support staff.

Filtering and virus protection:

- The school uses the LGfL filtering service (LightSpeed)

- Staff are to request the e-safety champion to unblock certain websites.

- Staff inform the ICT subject leader of suspected or actual computer virus.

6. Education and Training

In 21st Century society, staff and pupils need to digitally literate and aware of the benefits that use of technology can provide. However it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond. They should for example, be able to communicate safely and respectfully online, be

aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.

The three main areas of eSafety risk (as mentioned by Ofsted, 2013) that your school needs to be aware of are:

Area of Risk	**Example of Risk.**
Content: Children need to be taught that not all content is appropriate or from a reliable source.	• Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse. • Lifestyle websites, for example pro-anorexia/self harm/suicide sites. • Hate sites. • Content validation: how to check authenticity and accuracy of online content.
Contact: Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	• Grooming • Cyberbullying in all forms • Identity theft (including 'frape' – hacking Facebook profiles) and sharing passwords
Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to them selves and others.	• Privacy issues, including the disclosure of personal information, digital footprint and online reputation. • Health and well being-amount of time spent online (internet or gaming). • Sexting (sending and receiving of personally intimate images). • Copyright (little care or consideration for intellectual property or ownership-such as music or film).

6.1 eSafety across the curriculum

- It is vital that pupils are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' e-safety.

- We provide regular, planned e-safety teaching within a range of curriculum areas using the Lancashire ICT progression document.

- We have an additional focus in e-safety on safer internet day each year.

- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions

- Provision for children with special educational needs will be differentiated and on individual IEP's

- We ensure that pupils develop an understanding of the important of acceptable use policy and are encouraged to adopt safe and responsible use of ICT both within and outside of school.

- Children are reminded of safe internet use by use of classroom displays, safety rules, acceptable use policy when logging onto the school network.

6.2 eSafety – Raising staff awareness

- E-safety training for staff is updated on a regular basis to ensure they are aware of their responsibilities as outlined within this policy.

- Advice and training of individuals will be provided by ICT subject leader and /or Lancashire Teacher Advisors.

- E-safety training includes issues to make staff aware of their own personal safeguarding eg use of social networking sites.

- Training will be decided upon on the audit of staff needs carried out on a regular basis. The impact of training will be monitored on a yearly basis by the ICT subject leader.

- All staff are expected to promote and model responsible use of ICT and digital resources

- E-safety training is provided within an induction programme for all new staff, volunteers and students to ensure that they are fully understand both school's e-safety policy and acceptable use policy.

6.3 eSafety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Our school hold regular opportunities for parents and carers to be informed about e-safety, including the benefits and the risks of using various technologies.

- We hold meeting for parents to attend
- We use newsletters to promote e-safety awareness days
- We have links on the home of our website to Think You Know website.

6.4 eSafety – Raising Governors' awareness

The e-safety policy is regularly review and approved by the governing body. The governor with responsibility for Computing is kept up to date with regular meetings with the Computing subject leader discussions at governor meetings.

7 Monitoring Systems

The monitoring software that we use in school is Lightspeed.

The monitoring systems we have in place are as follows:

- We will regularly review our e-safety policy to ensure it is having the desired effect of keeping all users of technology safe.
- The e-safety champion will monitor reports created by Lightspeed of suspicious behaviour on a weekly basis.
- ALL STAFF are responsible for monitoring children's online behavior on a day to day basis whilst in school.

- E-safety incidents are to be recorded by adults who deal with the incident and will be monitored and reviewed by the e-safety champion.

- Appropriate procedures will be followed using the 'Responding to e-safety incident/escalation procedures' flow diagram.

- New technologies will be risk assessed before introducing them to children and the school network. As new technologies are introduced they will be included within the e-safety policy.

- The e-safety champion and ICT subject leader will analyse any incidents that occur to see if there is a recurring pattern eg specific days, times, classes, groups or individual children.

- These patterns will be addressed initially by the class teacher with circle time/PHSE sessions, discussions with parents. Then will follow more formal behaviour procedures set out in the Positive behaviour management policy.

- Staff, parents/carers, pupils and governors will be informed of any changes to e-safety policy and practice.

- The AUPs will be reviewed on a yearly basis and will include reference to current trends and new technologies.

e-Safety Incident Log

Date/Time of Incident	Type of Incident	Name of pupils and staff involved	System Details	Incident Details	Actions Taken

Responding to e-safety incident/escalation procedures