Lyneham
Primary School

E-Safety Policy

Member of staff responsible	Mr Johnathon Howard
Governor responsible	Mr Daniel Alexander
Date approved at Governing Body	November 2017
Frequency of policy review	Every 2 years
Date next review due	November 2019

Document Version Control

Issue Number	Issue Date	Summary of changes
1	Feb 2014	Annual review
2	Nov 2016	Review
3	Nov 2017	Policy review

1. Rationale

1.1 The internet and other technologies have the potential to offer many positive benefits to young people. As with everything, this is not without risk. We want young people to be able to fully exploit the benefits offered by ICT while doing so in a safe manner. Online messaging, social networking and mobile technology effectively mean that children can always be 'online'. Their social lives, and therefore their emotional development, are bound up in the use of these technologies.

1.2 In their e-safety guidance (September 2012) Ofsted states that the breadth of e-safety issues can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material
- contact: being subjected to harmful online interaction with other users
- conduct: personal online behaviour that increases the likelihood of, or causes harm.

1.3 The purpose of this policy is to ensure that the school community are kept aware of the risks as well as the benefits of technology and how to manage these risks and keep themselves and others safe. It details the measures that the school have put in place to support this.

1.4 The policy also aims to protect children from radicalisation and provide guidance on what to do if they believe a child is being radicalised or groomed online.

2. E-safety Working Group

2.1 E-safety is a priority across the school and reflected in the school improvement plan and in other relevant plans such as the Child Protection & Safeguarding planning. It is managed through the work of the e-safety working group.

2.2 E-safety developments and the e-safety policies are developed, reviewed and monitored, by our school e-safety working group which includes:

- ICT Subject Leader (Johnathon Howard)
- Head Teacher (John Read)
- Safeguarding Governor (Daniel Alexander)

2.3 Consultation with the whole school takes place through Student Council meetings, staff meetings, governor meetings and parent meetings.

3. Monitoring and Review

3.1 The policy is reviewed annually, but also in response to new technologies being introduced or incidents that have taken place. The e-safety working group monitor the impact of the policy using evidence from self-evaluation as identified below.

4. E-safety Self-evaluation

4.1 In order to understand the issues within our school community we gather and use a range of evidence to inform development of our practice, planning for the curriculum and planned professional development. Self-evaluation is conducted through:

- Logs of reported incidents
- Network monitoring data from the LA technical team
- Surveys / questionnaires of students, parents / carers, and staff including non-teaching staff
- E-safety self-evaluation checklist and local authority safeguarding audit
- Pupil and parent views are regularly sought to inform developments

4.2 The South West Grid for Learning 360 degree safe online tool is also used annually as a benchmark to enable us to monitor our development towards more effective practice.

5. Scope of the Policy

5.1 This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems. It applies to systems in school and out of school where activities have been set by the school or are using school online systems.

5.2 The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, inform parents / carers of known incidents of inappropriate e-safety behaviour that take place out of school.

5.3 This policy should be considered in conjunction with the following policies and documents which it complements:

- Mobile Device Pupil User Agreement for pupils and parents / carers which outlines acceptable behaviours when using technology
- Positive Behaviour Management Policy which outlines the procedures, rewards and sanctions associated with online behaviour, including cyber-bullying.
- Anti-bullying Policy which details how issues of online bullying (cyber-bullying) will be dealt with.
- Curriculum Policy which outlines how ICT is used throughout the school.

6. Roles and Responsibilities

6.1 These are clearly detailed in Appendix 1 for all members of the school community. They are briefly summarised below.

- **The Head Teacher** (John Read) is responsible for ensuring the safety (including online safety) of members of the school community.
- **The designated persons for child protection** (John Read and Kate McFarlane) are trained in e-safety issues and are aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate online contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.
- **Governors** are responsible for approval of the E-Safety Policy and for reviewing effectiveness of the policy and this will be carried out by the School Improvement Committee. We have an E-Safety governor (Daniel Alexander) who meets regularly with the e-safety lead (Johnathon Howard) to monitor developments and feeds back to governors.
- **The e-safety lead** takes day to day responsibility for e-safety issues, leads our e-safety working group, liaises with technical support and the e-safety governor, and ensures that all staff are trained and fully aware of policies and procedures. The e-safety lead is responsible for reviewing and developing e-safety procedures, including training, to make sure that they have a positive impact on pupils' knowledge and understanding.
- **Teachers and support staff** must ensure that they are aware of e-safety issues, policy and practices and that they have understood and signed the Staff Acceptable Use Policy.
- **Children** are also responsible for using ICT as outlined in the Mobile Device Pupil User Agreement Policy which they sign, or in the case of key stage 1 pupils, their parents sign. Parents have responsibility for ensuring that they read and understand the Mobile Device Pupil User Agreement Policy and endorse this by signing it.
- **Technical support** the school monitors the work of external technical support staff and ensures that they are fully aware of this policy. The technical support advisor (Oakford Technology) is responsible for ensuring that school infrastructure is secure, and not open to misuse or attack. They ensure that the school meets the requirements of this policy. Users can only access the school's network through an enforced password protection policy, in which passwords are regularly changed. Technical support staff inform the SWGfL about any filtering issues. Appendix 2 provides a detailed summary of the roles of technical support team where the local authority supports a school. This can also be used as a checklist with other support providers to ensure that these aspects are covered.

7. Education of Pupils and the Curriculum

7.1 Whilst regulation and technical solutions are important, their use must be balanced by educating learners to take a responsible approach. The education of students in e-safety is an essential part of our school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

- We have an age-related e-safety curriculum that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm, understand how to manage risk, and how to take responsibility for their own and others safety and how to be responsible users of technology.
- E-safety is embedded in all relevant areas of the curriculum including research in History/Geography, publishing in English, social skills in PSHE, data handling in maths and core skills in ICT.
- The e-safety scheme of work identifies for each year group progression statements, learning outcomes, processes, skills, vocabulary, suggested software and web links, sample activities and assessment activities.
- Key e-safety messages are reinforced through assemblies.
- Reference is made to e-safety in the Home-School Agreement for all parties.
- Pupils are given age appropriate support to search safely and to evaluate the content that they access online. Processes are in place for dealing with any unsuitable material that is found in internet searches. Staff are vigilant in monitoring the content of the websites the children visit and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- Pupils are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information. Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Our Positive Behaviour Management Policy is also used to reinforce online behaviour with positive sanctions being used to reward positive and responsible use of ICT.
- Staff use their teacher laptop to share with pupils how to deal with issues outside school where there may be no filtering.
- Teachers monitor ICT use during lessons.

8. Parents / Carers

8.1 Parents and carers may have only a limited understanding of e-safety issues and may be unaware of risks and what to do about them. They have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The school supports parents to do this by:

- Providing clear acceptable use policy guidance and regular newsletter and web site pages
- Inviting parents to attend activities such as e-safety week and e-safety assemblies
- Offering workshops for parents / children teaching parents about safe use of technologies

9. Education and Training – Staff and Governors

9.1 There is a planned programme of e-safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the acceptable use policies.

- An audit of the e-safety training needs of all staff is carried out annually and this is used to plan professional development.
- All new staff receive e-safety training as part of their induction programme.
- The e-safety leader receives regular updates and training sessions and through regular e-safety updates from the local authority.
- This E-Safety Policy is discussed in staff meetings.
- The e-safety leader provides advice/guidance and training as required to individuals as required and seeks advice on issues where required.
- Staff act as good role models for pupils in their own use of ICT.
- Governors are included in e-safety awareness sessions and training.

10. Use of Digital and Video Images

10.1 Digital imaging technologies create significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are reported incidents of employers carrying out internet searches for information about potential and existing employees. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm.

10.2 Parents sign a consent form which allows photographs of their child to be used for publications and on the web site. Photographs are carefully chosen and any published photographs or videos of pupils will not be used alongside full names.

11. Data Protection

11.1 The school complies with the 1998 Data Protection Act which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant
- Accurate
- Kept no longer than necessary
- Processed in accordance with the data subject's rights
- Secure and only transferred to others with adequate protection

11.2 Staff ensure that they:

- Ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers / devices, ensuring that they are properly logged off at the end of a session using personal data
- Transfer data using encryption and secure password protected devices / memory sticks
- Delete personal data from portable devices once they have finished with it

12. Passwords

12.1 All users of ICT systems log in with an individual user name to ensure that all only have access to the data they have a right to access. Passwords for staff are regularly changed. Passwords are managed by the technical support provider and any changes are logged.

13. Filtering

13.1 Filtering is provided through SWGfL internet service. Any changes to filtering are requested and managed through the ICT Subject Leader.

14. Use of Personal Equipment in School

14.1 Staff have use of school cameras and devices so use of personal devices images and video is not necessary or allowed.

14.2 Staff personal mobile phones should not be used to store contact details of parents and pupils. There is a school mobile phone which should be used for school trips.

15. Communications Technologies

15.1 A wide range of communications technologies have the potential to enhance learning.

15.2 The official school email service is used for communications between staff, and with parents / carers, as it is regarded as safe and secure, provides an effective audit trail and is monitored.

15.3 The school ensures that, where communication technologies are used then tools are chosen that enable staff to monitor their use, for example, moderated blogs, e-mail which can be monitored and secure areas for sharing information. This is sometimes through the use of group and class accounts for ease of monitoring.

16. Reporting and Dealing with Incidents

16.1 There are activities that are inappropriate in a school context and users should not engage in these activities in school or outside school when using school systems. These are detailed in Appendix 3.

16.2 We expect all members of the school community to be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy take place, through careless, irresponsible or, very rarely, deliberate misuse. School-based online reporting processes are clearly in place and understood by the whole school. They are detailed in Appendix 4 and are summarised as follows:

- Pupils report any issue to their teacher or other adult
- Staff must immediately report any issue to the e-safety lead and, in the case of possible child protection issues, to the Head Teacher or School Business Manager who are responsible for child protection
- Any issues that can not be resolved by the teacher are escalated to involve the Head Teacher
- The e-safety lead must report any issues to do with filtering to the local authority help desk. E-safety issues can also be escalated and should be reported to the appropriate local authority staff

- If any misuse appears to involve illegal activity the SWGfL flow chart below is consulted and followed, in particular the sections on reporting the incident to the police and the preservation of evidence, illegal activity would include:
    - child sexual abuse images
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- The e-safety lead is responsible for ensuring staff are kept fully informed about any issues and their resolution

16.3 If members of staff suspect that any misuse might have taken place it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL 'Procedure for Reviewing Internet Sites for Suspected Harassment and Distress' will be followed. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a 'clean' designated computer. The school is more likely to encounter incidents that involve inappropriate rather than illegal misuse.

Appendix 1: Roles and Responsibilities

The following roles and responsibilities have been allocated and agreed across the school.

Role	Responsibility
Governors	Approve and review the effectiveness of the E-Safety Policy and Mobile Device Pupil Agreement. E-Safety Governor works with the E-Safety Leader to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering and then reports to Governors
Head Teacher And Senior Leaders	Ensure that all staff receive suitable CPD to carry out their e-safety roles and sufficient resource is allocated. Ensure that there is a system in place for monitoring e-safety. Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff. Inform the local authority about any serious e-safety issues including filtering. Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.
E-Safety Leader	Lead the e-safety working group and dealing with day to day e-safety issues. Lead role in establishing / reviewing e-safety policies / documents. Ensure all staff are aware of the procedures outlined in policies. Provide and/or brokering training and advice for staff. Attend updaters with the LA e-safety staff. Liaise with technical staff. Deal with and log e-safety incidents including changes to filtering. Meet with E-Safety Governor to regularly monitor e-safety developments. Report regularly to Senior Leadership Team.
Curriculum Leaders	Ensure e-safety is reflected in teaching programmes where relevant eg: anti bullying English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	Participate in any training and awareness raising sessions. Have read, understood and signed the Staff Acceptable Use Agreement (AUP) Act in accordance with the AUP and e-safety policy. Report any suspected misuse or problem to the E-Safety Co-ordinator Monitor ICT activity in lessons, extra curricular and extended school activities.
Pupils	Participate in e-safety activities, follow the Mobile Device Pupil User Agreement and report any suspected misuse. Understand that the E-Safety Policy covers actions out of school that are related to their membership of the school.
Parents and Carers	Endorse (by signature) the Home School Agreement Policy. Ensure that their child / children follow Mobile Device Pupil User Agreement rules at home. Discuss e-safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet.

	Access the school website in accordance with the relevant school Mobile Device Pupil User Agreement. Keep up to date with issues through school updates and attendance at events.
Technical Support Provider	Ensure the school's ICT infrastructure is secure in accordance with Becta guidelines and is not open to misuse or malicious attack. Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data. Inform the Head Teacher of issues relating to the filtering applied by the Grid. Keep up to date with e-safety technical information and update others as relevant. Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction. Ensure monitoring software / systems are implemented and updated. Ensure all security updates / patches are applied (including up to date anti-virus definitions, window updates) and that reasonable attempts are made to prevent spyware and malware.

Appendix 2 – Technical Support Provider Guidelines

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- School ICT systems are managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and relevant Local Authority E-Safety guidance.
- There are regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT systems.
- All users are provided with an individual username and password and are responsible for the security of their username and password.
- Where the local authority provides curriculum technical support the 'administrator' passwords for the school are not held by the school and the local authority are responsible for their security and any implications of their use and have an agreement in place for this.
- The school maintains and supports the managed filtering service provided by SWGfL.
- In the event of the school technician needing to make requested changes to filtering, including removing sites from the filtered list, this is logged and approved by the ICT Subject Lead before being carried out.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this.
- Actual / potential e-safety incidents are documented and reported immediately to the E-Safety Leader who will arrange for these to be dealt with immediately.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual work stations are protected by up to date virus software.
- Personal data can not be sent over the internet via e-mail or taken off the school site. This is done through secure file transfer or using encrypted memory sticks.
- There are a number of 'supply' log ins that can be used to provide temporary access on to the school system for trainee teachers and visitors. These are allocated to individuals and a log is kept of their use. Regular visitors / supply teachers have their own log in.
- Downloading of executable files can cause issues and compromise security and permission should be sought from the provider for this to happen.
- Staff are allowed to use their school laptop at home for planning purposes. An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.

- Staff should not install any programmes on a school workstation / portable device without prior permission from the ICT Subject Leader and advice sought from technical support.
- Staff should not be using personal memory sticks / external hard drives on school equipment unless with prior agreement and the device has been checked for viruses.

Appendix 3 – Unsuitable / Inappropriate Activities

The school believes that the activities referred to below are inappropriate in school and that users should not engage in these activities in school or outside when using school equipment or systems.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images					X
	Promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation					X
	Adult material that potentially breaches the Obscene Publications Act in the UK					X
	Criminally racist material in UK					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Promotion of racial or religious hatred				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Any other information which may be offensive to colleagues, breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)				X		
On-line gambling					X	
On-line shopping / commerce				X		
File sharing					X	
Recreational use of Social Networking during directed time (staff)						
Use of social networking sites apart from where sanctioned for specific educational use by Head Teacher					X	
Use of video broadcasting e.g. Youtube				X		