LUCK LANE
A SHARE Primary Academy

E-Safety
June 2022

Introduction
This e-Safety policy outlines practice which aims to ensure the safe use of the technologies such as iPads, mobile phones, computers and other devices with wired or wireless connectivity to the internet. The policy highlights the need to educate children and young people about the benefits and risks of using new technologies both in and outside of school. It also provides safeguards, procedures and rules to guide staff, pupils and visitors in their online experiences.

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

- A comprehensive, agreed and implemented e-Safety policy
- Responsible IT use by staff, pupils or visitors
- Secure filtering at school and off site
- Understanding of the capabilities of devices and software

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 National 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

School internet access should only be used by pupils, teachers and visitors to support learning. All use should be educational use, use related to teaching and learning, use related to staff job descriptions and in-line with the ethos of the school.

Pupils will be taught safe internet use through the SMART rules model (https://www.childnet.com/young-people/primary/get-smart).
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 taught how to evaluate internet content. Staff should ensure that their own and their pupils use of internet derived materials 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 concerns verbally to staff and digitally to organisations (i.e. CEOP).

Managing Internet Access
Internet filtering and security is currently run and delivered through a system controlled and monitored by the central Tech Team. 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 Tech Team as soon as possible. Security concerns or changes must be reported to line managers, Head Teacher and Governors, if the need arises.

Authorising Internet access
Pupil instruction in responsible and safe use should precede any internet access and all pupils must abide by the school's e-safety Rules. The e-safety Rules will also be displayed clearly in all networked rooms.
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.

E-mail/Messaging
Pupils do not use email services. All devices are 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.

Pupils may only use messaging facilities that teachers can administrate, moderate and monitor (i.e. Dojo). Staff have admin rights to check and monitor these. Pupils must immediately tell a teacher if they receive an offensive message.

All communication should be approved by and shown to an adult.

E-mails written as part of a lesson, for example, to send to an external organisation or an author, should be written carefully and authorised by teacher before being sent by a teacher. This should not lead to pupils owning, creating or maintaining an email address that could be used by them in future for private communication.

Staff are provided with an email address to use for school correspondence. This must be used in line with data protection law and guidance, secure passwords must be set and maintained. All staff should treat incoming e-mail as suspicious and attachments not opened unless the author is known.

Dialogue between pupils and teachers outside Dojo is not allowed and any email correspondence between a teacher and parent should be 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. School email addresses can only be held by current staff and on termination of duties with school, the address will be deleted.

Text messages to parents and pupils can only be sent via the school office and never from staff personal emails or mobiles. Staff and pupil email addresses/online files and folders/accounts created by school remain the property of the school and relevant members of staff can access these for viewing and monitoring.

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 by name. Where possible, group photographs will be used rather than full-face photos of individual children. Pupils' full names will not be used on the internet 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 internet
.
Teachers can not publish images of pupils or their work, discuss pupils or publish information about them outside of the school's own platforms including on their own social media or private messaging. They are responsible for complying with the GDPR regulations and policies. A list of pupils that cannot be photographed will be listed for staff and retained by the school. Pupils cannot consent to photographs being taken if parents have objected.

Social networking and personal publishing
The school will block access to well-known social networking sites using the filter and via proxy. Upon discovering that access to social networking becomes possible, pupils and staff must report this immediately to senior leadership or the central tech team. Staff must educate pupils in the dangers of using social media as part of their e-safety education. Education in the safe use of social media does not suggest or imply that pupils should be allowed to access social media sites or advocate use. Pupils must be taught e-safety in line with the computing programme of study using the SMART rules. These must be displayed in every classroom.
https://www.childnet.com/young-people/primary/get-smart

Staff are advised to regularly review their personal 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 a 'friend';
- Reviewing 'friend lists' regularly;
- Regularly checking the content of profiles;
- Avoiding publishing material about place/s of work;
- Use of strong passwords for any social networking systems;
- Ensuring profiles are set to 'secure' or 'private'.

- Never adding a Millbridge pupils or parents to friends lists;
- If a request from a pupil or parent is received, senior leaders should be contacted.
- It is forbidden for staff to add pupil's family members to social media sites even if they have a connection outside of school. Any connections thought to be exceptions to this should be discussed with line managers.

The use of social media, forums and internet platforms is ever evolving and it is the responsibility of staff to ensure they are keeping information appropriate and private. Staff are entirely responsible for their online activities and although the school will offer advice and guidance regarding social media, it remains the responsibility of all staff to ensure that their 'digital footprint' is in line with the expectations of their role. Staff are responsible for all persons posting under an account owned by them, i.e. friends posting on their behalf on social media accounts.
Staff should report any concerns about others in-line with school policies.

Any communication between staff and children within school platforms, i.e. Dojo, should clearly observe professional boundaries. Staff should not share any personal information. They should not request or respond to any requests for personal information from pupils other than that which is appropriate as part of their professional role. Staff should ensure that all communications are transparent, education focused, open to scrutiny and in line with Share MAT 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

Managing filtering
The school will work closely with the central tech team, who operate a comprehensive filtering system, which protects schools from accessing unsuitable material. However, due to the international scale, immediate 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 device.

Incidents of inappropriate material accessed, should be evidenced and reported, in-line with the school safeguarding and behaviour policies.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Staff may have access to some sites which pupils cannot access, such as You Tube for educational purposes, but content must be checked carefully prior to being used in class.

Managing personal technologies
Technologies such as mobile phones with 4G wireless internet access and games systems not belonging to school are not linked to the school filtering systems and present a route to undesirable material and communications and are therefore forbidden. 'Hot-spotting' devices in school is not allowed other than for testing the proxy on a device by IT staff. The use of portable media such as memory sticks must be avoided and can be inspected by school staff regardless of ownership so should not contain personal information.

Staff can be given the wifi passwords but must not put personal devices i.e. mobiles or devices not belonging to school onto any school network.

Staff should not allow others (i.e. children, partners, friends) use of their school devices.

Pupils' mobile phones will not be permitted in school unless for emergency (i.e. Y5/6 pupils who walk home alone), 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.

Staff can only use cameras that belong to school. The use of personal cameras, including those on mobile phones, is forbidden. The use of accounts which sync and could transfer data from personal devices to school devices must be managed by staff. Any data on a school device or cloud platform can be accessed by the central tech team without permission or the knowledge of the staff member.

Personal devices should never be used in front of pupils.

Public computers (such as libraries or cafes) should not be used to access school information remotely due to the high-risk of data exchange.

Personal passwords must be used only for personal devices. Any passwords related to school devices or accounts must be provided to senior leaders on request and therefore should be unique to school. Any breach of the school's policy could lead to disciplinary action.

Introducing the E-Safety Policy to pupils

E-safety rules will be discussed with all pupils in computing lessons, whole school assemblies, class assemblies and PSHE sessions. Pupils will be informed that internet use will be monitored and appropriately followed up if used inappropriately.

Millbridge is a member of National Online Safety:
https://nationalonlinesafety.com/

This means we teachers have access to lessons and teaching materials centred around aspects of e-safety. All members of staff have access to a wide variety of training courses to help develop up-to-date knowledge and understanding of e-safety. Parents can also set up accounts and school can sign-post groups or individuals to training courses to help them further understand e-safety at home.

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 fact files and the PSHE curriculum. The school participates in the nationwide safer internet day:
https://www.saferinternet.org.uk/safer-internet-day/

Enlisting parents' support

Parents' attention will be drawn to the School E-Safety Policy in newsletters, on Dojo and on the website.
The app https://www.internetmatters.org/hub/esafety-news/new-e-safety-app-for- parents-and-children/ will be shared.