STILLNESS INFANT SCHOOL

e-Safety
Internet Policy Document
September 2021

Cameron McKinlay

Who will write and review the policy?

- The school e-Safety Coordinator is Cameron McKinlay who has written our e–Safety Policy, building on the KCC e–Safety Policy and government guidance. It has been agreed by the Senior Leadership Team and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually. Parents will be requested to sign an e–Safety/internet agreement as part of the Home School Agreement.

Why is Internet use important?

- Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school, especially through apps and need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

- Access to world-wide educational resources including museums and art galleries;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations.

How will we achieve compliance and meet obligations?

- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the Internet and apps that use it to function in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate Internet content and keep themselves safe?

- Within EYFS/Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- In Key Stage 1 some searching by using specifically approved key words (such as 'rain forest animals' or 'lion facts') will be used under the supervision of class teacher or other school adults.
- The teacher leading any initial internet based sessions will explain to the children that the internet, while being an amazing resource, does contain some information that is not necessarily true and some information or pictures that can be distressing. This will also include any material that could, however inadvertently, contribute to radicalisation of any kind, i.e.; violent political radicalisation not just extreme religious radicalisation. The children will be told that the school's internet safety programs should make sure that they don't read or see anything upsetting, but if they do read or see anything upsetting they are to move away from the screen, turn it off if possible or if on an iPad to put it down and let an adult know straight away.

- Any such incident will be investigated by the ICT coordinator who can take any necessary steps, such as making sure that site is blocked. The borough wide 'safety-net' is very through and the risk of the children being able to access anything untoward is small.
- To minimize risk, the children are taught to only go to pre-approved sites and when they are searching for facts (such as rain forest facts) on the internet in Year Two, how to make sure their searches are very specific. The children will be reminded of these key points at the start of any session that will involve the internet and will be mentioned in teachers' planning. The children are taught that when using apps, these can take the children onto the internet and not to click on any links unless they've checked with an adult first.
- The children will be shown the acceptable Internet use policy/posters. Although it is hugely unlikely that the children would contravene the policy, it is good to remind them that it is there to keep themselves and the school systems safe.

How should personal data be protected?
- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2016, for more details see our data protection policy.
- All school PCs are password protected, with individual passwords for members of staff and bulk passwords for pupils, usually on a class by class basis. Pupil data (such as their Word or PowerPoint documents) and staff data will be kept in separate area of the school's data storage.
- Any photographs taken for school business will be deleted upon uploading and if they are to be stored, stored in a password protected area of the school's data storage. Permission will be gained for photographs being used on either the school website or Instagram.
- Any sensitive files being transported between home and school (typically individual pupil reports or whole class/school data) should be transported on password protected laptops, password protected memory sticks or the files themselves to have passwords placed upon them.

What will be the E-safety expectations for staff members?
- Pictures should be uploaded regularly to password protected areas of the shared drive and deleted from the device at the same time.
- Any sensitive data (this could be whole class data or individual reports) transported between school and home should be transported on password protected laptops, password protected memory sticks or the files themselves have passwords placed upon them.
- Any emails sent from your school 'staff mail' should be considered to be as official as sending a letter on school headed paper. Please remember to be respectful at all times when using your school email.
- Social media should not be used to criticise or undermine other members of staff, children, parents or the school as a whole. Anything posted on social media should be suitable for posting on the communication board in the staffroom.

How will Internet access be authorised?
- Parents will be asked to sign and return a consent form for pupil access.

How will risks be assessed?
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate. Methods to identify, assess and minimise risks will be reviewed regularly.
- Children's understanding of e-safety will be monitored by class teachers and monitored through pupil voice via the school council.

How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use both professionally and personally will be provided as required. To protect all staff and pupils, the school will implement Acceptable Use Policies/e-safety expectations; see below.
- The e–Safety Policy will be formally provided to and discussed with all members of teaching staff at a specific staff meeting with all teachers in attendance and at follow up meetings with all support staff.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School e–Safety Policy in newsletters and on the school website and mentioned during our annual parental meeting during Internet Safety Week.

Stillness Infant School

Responsible Internet Use

We use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- **I will ask permission before entering any new Web site, unless my teacher has already approved that site.**

- **I will only search the Internet with 'key words' provided, unless I have asked a school adult.**

- **I will not look at or delete other people's files.**

- **I will not bring memory sticks into school without permission.**

- **I will not use Internet chat.**

- **If I see anything I am unhappy with or I receive messages I do not like, I will tell a school adult immediately.**

- **I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.**

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Stillness Infant School

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Stillness Infant School is providing supervised access to the Internet. We believe that the use of the World Wide Web is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use, and sign and return the consent form so that your child may use Internet at school.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Yours sincerely

Consent Form

Stillness Infant School
Responsible Internet Use
Please complete, sign and return to the school office

Pupil:	*Class:*

Parent's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	*Date:*
Please print name:	

E-safety expectations for staff members

- Pictures of children only to be taken on school devices or school approved devices, this could be visiting photographers' cameras for instance.

- Pictures should be uploaded regularly to password protected areas of the shared drive and deleted from the device at the same time.

- Personal mobile phones or other similar devices that can take pictures should be left in a secure area during hours when the children are on site.

- Any sensitive data (this could be whole class data or individual reports) transported between school and home should be transported on password protected laptops, password protected memory sticks or the files themselves have passwords placed upon them.

- Any emails sent from your school 'staff mail' should be considered to be as official as sending a letter on school headed paper. Please remember to be respectful at all times when using your school email.

- Social media should not be used to criticise or undermine other members of staff, children, parents or the school as a whole. Anything posted on social media should be suitable for posting on the communication board in the staffroom. Contraventions will be taken seriously and legal or disciplinary action will be taken.

- Always be aware of the level of privacy settings commination platforms have. For instance; Facebook has very high privacy settings that can be put in place, whereas, Twitter does not.