STAINES PREPARATORY SCHOOL

E-SAFETY POLICY

(On-line Safety)

Review Procedure:	**Annually for September**
Person Responsible:	**Designated Safeguarding Lead**
Reviewed by: Designated Safeguarding Lead (DSL)	**September 2018**
Approved by: Headmistress	**September 2018**
Approved by: Governors	**September 2018**

SPS E-safety Policy

The E-safety Policy relates to other policies including those for Computing, Anti Bullying, Child Protection and Computing Acceptable Use.

- The school's E-safety coordinator is the Designated Safeguarding Lead.
- Our E-safety policy has been written by the school, building on best practice and government guidance.

The E-safety policy and its implementation will be reviewed annually.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
• **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Teaching and Learning

- 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 curriculum and a necessary tool for staff and pupils.

The school Internet access includes filtering appropriate to primary school pupils and is reviewed regularly, including ensuring that children are safe from terrorist and extremist material (as required by the Prevent Duty) and inappropriate material when accessing the internet at School. Advice has been taken from UK Safer Internet Centre: appropriate filtering and monitoring

- Pupils will be taught what Internet access is acceptable.

- Pupils will be given clear learning 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.

- Pupils will be shown how to publish and present information appropriately to a wider audience.

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

- Younger pupils will be directed to accurate sources of information and older 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 to report unpleasant Internet content to a teacher or appropriate adult.

Managing Internet Access
Systems Security

- School ICT systems security will be reviewed regularly.

- Virus protection will be updated regularly.

Managing filtering

- If staff or pupils come across inappropriate on-line materials, the site must be reported to the ICT Technical Manager.

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

Email

- Pupils may only use approved e-mail accounts on the school system. Pupils in Years 3 to 6 have access to a school e-mail account, which is restricted to use only for school projects covered within the Computing Curriculum.

- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone, this will be taught during lessons.

- Incoming e-mail should be regarded as suspicious and attachments not opened unless the author is known.

- The forwarding of chain letters is not permitted.

- Pupils must immediately tell a teacher if they receive offensive e-mail from any person known or unknown to them.

- The school will instruct pupils how to present e-mail to external bodies and this will be controlled by a teacher.

- Communication between staff and pupils must only take place within the school's learning platform (*eSchools*) and will be monitored.

Published content and the school website

- The contact details on the school website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

- The Headmistress or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

- Photographs that include pupils will be selected carefully and in accordance with the wishes of individual parents.

- Pupils' full names will be avoided on the website or learning platform, including in blogs, forums or wikis.

- At school, pupils may only upload files/images to the learning platform (*eSchools*), if a teacher gives permission and at home, only if approved by an adult. Pupils must only upload examples

of work created by themselves.

Social Networking

- Access to social networking sites is not permitted in school. However, the school will advise pupils about their safe use e.g. use of passwords and appropriate age limits. Staff have received training on peer on peer abuse and 'sexting' to develop their awareness of identifying concerning behaviours which may be linked to sexting. The training ensures that staff know how to respond to concerns in line with the school's Child Protection policy.

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

- Pupils will be advised to use nicknames and avatars, when using social networking sites.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.

- Mobile phones and associated cameras are not normally permitted to be used by pupils at school. In the 'in extremis' event that a mobile phone is permitted, the pupils are supervised when using it and the sending of abusive or inappropriate messages is forbidden; the children will be taught to report such incidents if they occur. Pupils will also be advised on the safe use of mobile phones when outside of school (in line with the school's ICT Acceptable Use policy).

- Staff will use a school phone, where contact with parents is required and follow the school's Mobile Phone policy when using a mobile phone at school.

Protecting Personal Data

- We follow the General Data Protection Regulations enforced in May 2018 to record any data shared through use of the internet for example, online systems such as Classroom Monitor, Tapestry, eSchools.

Policy Decisions

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

- In Pre-Prep and Lower School, access to the Internet will be closely monitored by the class Teacher and class LSA.

Community Use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school's E-safety policy.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale, linked Internet content and the risk of 'over-blocking', it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access but will ensure that such instances are dealt with appropriately with guidance from either the Rewards and Sanctions policy or Child Protection policy.

Handling E-safety 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 Headmistress.
- 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.

Communications Policy
Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils through the ICT Acceptable Use policy.
- E-safety rules will be displayed in appropriate places within the school, and taught as part of the Computing Curriculum.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils.

Staff and the E-safety Policy

- All staff will be given the school E-safety Policy and its importance explained. Staff are also aware of the Staff Behaviour Policy and Mobile Phone and Devices Policy. Discretion and professional conduct is considered essential.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.

Enlisting Parents' Support

- Parents' and carers' attention will be drawn to the school E-safety Policy on the school website.
- Parents and carers will from time to time be provided with additional information on E-safety.

Information and support

There is a wealth of information available to support schools, colleges and parents to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Organisation/Resource	**What it does/provides**
thinkuknow	NCA CEOPs advice on online safety
disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online
parentzone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images

educateagainsthate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
the use of social media for online radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
UKCCIS	The UK Council for Child Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
net-aware	NSPCC advice for parents
commonsensemedia	Independent reviews, age ratings, & other information about all types of media for children and their parents
searching screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
lgfl	Advice and resources from the London Grid for Learning

This policy also applies to the Early Years Foundation Stage