

	<p>SLINGSBY SCHOOL</p> <h1>E–Safety Policy</h1>	<p>Date for Review</p> <p>September 2018</p>
---	---	--

What is Internet Safety?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

E-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care', which applies to everyone working with children.

Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have.

Writing and reviewing the E-safety policy

The E-Safety Policy relates to other policies including those for ICT and for child protection. The school's ICT Co-ordinator will also act as E-Safety Coordinator. Our e-Safety Policy has been written by the school, building on the NYCC E-Safety Policy and government guidance. It has been agreed by senior management and approved by governors. The E-Safety Policy and its implementation will be reviewed regularly.

Teaching and Learning

Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils may use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use will enhance learning

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear 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 taught how to evaluate Internet content

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.

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly.

Virus protection is updated regularly.

Advice on security strategies will be monitored on the School's ICT web page and clarification sought as necessary.

Parents will be made aware of the e-safety policy.

Pupils are told to:

- Only access websites which you have been told/have permission to do so.
- Never pass on personal information about yourself over the internet.
- Always tell an adult if you come across something inappropriate on the internet so that it can be recorded and acted upon.

E-mail

Pupils may only use approved e-mail accounts on the school system and email usage should be supervised and monitored by a staff member.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

Published content and the school web site

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

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Social networking and personal publishing

The school will block/filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind that may identify them or their location.

Pupils will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

The school will work with NYCC, School's ICT and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the Head Teacher.

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

Managing emerging technologies

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

Pupils' mobile phones are to be handed into the Office Manager on arrival and collected after school. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

For Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

For Key Stage 2, children are made aware of the Internet safety steps that are to be taken prior to Internet use and that children never access the Internet without a suitable adult present.

Parents will be asked to sign and return an acknowledgement form.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, 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.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

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 head teacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Misuse of social media by a parent will be reported to the legal department of NYCC and in some cases to the police.

Communications Policy

Introducing the e-safety policy to pupils

E-safety rules will be discussed with pupils.

Pupils will be informed that network, Internet and DB Primary use will be monitored.

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored. Discretion and professional conduct is essential.

All parents will be issued with a social media policy.

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters (as and when appropriate), the school brochure and on the school Web site.

Parents will also be provided with a social media policy and misuse will result in legal action.