Old Park Primary School

reaching for success

E SAFETY POLICY

Reviewed July 2021

Next planned review July 2022

Writing and reviewing the E-safety policy

The E-Safety Policy relates to other policies including Computing, Anti-bullying, Acceptable Use and Social Media and Child Protection and Safeguarding.

The school's Computing Co-ordinator will also act as E-Safety Co-ordinator.

Our E-Safety Policy has been agreed by senior management and approved by governors. The E-Safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Why internet use is important

The internet is an essential additional learning tool within education and 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.

Internet use will enhance learning

The school internet access is designed for pupil use. Pupils have access to a variety of computing equipment to enable them to access the internet for their learning and prepare them for secondary education. Pupils will be taught how to use the internet safely to find relevant and useful sources to enhance their learning.

Pupils will be taught how to evaluate Internet content

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval, and evaluation.

Pupils and parent/carers from all year groups will sign an acceptable user policy agreement.

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

Information system security

School ICT systems security will be reviewed regularly by the ICT technician from T&W

Service Provider (T&W) filters information using Smoothwall (filtering system).

WiFi access is password protected.

Staff must use Senso to monitor and control what pupils are typing/accessing during use of computers/laptops to meet safeguarding responsibilities.

Meraki management solution is used to control what pupils are accessing on the school iPads maintains the safe use of technology.

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 an offensive e-mail.

Pupils must not forward chain letters/emails.

Pupils must not reveal personal details of themselves or others in e-mail communication.

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.

Incoming email from an unknown author should be treated as possibly suspicious and attachments not opened.

Published content and the school website

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

The headteacher and website administrator take editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully.

Pupils' full names will not be used anywhere on the website in association with photographs or blogs.

Written permission from parents or carers will be obtained as part of the admission process before photographs of pupils are published on the school website.

Social networking and personal publishing

The school has a social media policy.

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

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

Pupils and parents 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 the LA, DfE 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 ICT administrator.

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

Protecting personal data

Personal data will be processed in accordance with the requirements of GDPR legislation (or equivalent UK legislation)

Authorising Internet access

All staff must read and sign the 'Acceptable Use Agreement' before using any school ICT resource.

Written permission from parents or carers will be obtained as part of the admission process for their child to access the internet.

The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up to date, for instance, a member of staff may leave or a pupil's access be withdrawn.

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. Neither the school nor LA can 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.

Pupils are taught to report inappropriate material to an adult so that action can be taken. This will include making a note of the website and any links, informing the ICT administrator who will then take action to block the website. A discussion will take place with the pupil, and parents, when appropriate.

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 Headteacher.

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.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues

Introducing the e-safety policy to pupils

E-safety rules will be discussed with the pupils at the start of each year.

Pupils will be informed that network and internet use will be monitored.

Pupils will be informed that their internet use is monitored and traced to the individual user and that anyone not using the internet appropriately will be denied access to using the internet.

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 and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy on the school website.

Parents have access from our school website to e-safety tools and website links.