Parklands
Educate Together

Online Safety Procedures

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. This policy details the procedures in place to support safe and responsible use of the internet by all members of the school community.

We would like to acknowledge that SWGfL model policy was used during the development of these procedures. Further information from SWGfL can be found here http://swgfl.org.uk/products-services/esafety/resources/creating-an-esafety-policy

This Online Safety Procedures work in conjunction with other policies, including those for Computing and Safeguarding. Online safety is the responsibility of every member of school staff, with the Safeguarding team being responsible for issues or concerns arising from the use of technology as with other concerns.

Teaching staff:

- have an up-to-date awareness of online safety matters, know the current policy and follow good practice guidelines. They are kept up-to-date with information through staff INSET, guidance information and self- study.
- abide by the Acceptable Use of ICT policy and the staff Code of Conduct
- report any suspected misuse, by pupil or adult, to the Headteacher, Deputy or School Administrator as soon as possible
- ensure that any online communication with pupils or parents is professional
- ensure that online safety is planned for and embedded into their teaching
- monitor the use of digital technologies, mobile devices, cameras etc by pupils and adults and implement policies where applicable

All staff will:

- receive online safety training which is updated as new information or technologies arise. Training is refreshed each year as part of the annual safeguarding updates from the school, Trust and Local Authority.
- respond to online safety concerns involving staff or pupils promptly.
- when new, receive online safety information as part of their induction including Acceptable Use of ICT

- be provided with advice, guidance or training as requested or as identified through performance management procedures.

The Internet is an essential element in 21st century 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. The purpose of the Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

Internet access is an entitlement for students who show a responsible and mature approach to its use. They 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.

The school Internet access is planned expressly for pupils' use and includes filtering appropriate to the age of pupils.

Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use within the Computing, PSHE and Learn Together curriculum, although may not be exclusively to these subjects.

Principles of Teaching Online safety

Internet access will be planned to enrich and extend learning activities for all age groups.

Staff will guide pupils in on-line activities that supports the learning outcomes planned for the pupils' age and maturity.

Pupils are 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
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is part of every subject.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported, where appropriate, to SLT or in their absence, directly to Soltech support.
- The School ensures that the use of Internet derived materials by staff and by pupils complies with copyright law.

Managing Internet access

The security of the school information systems will be reviewed regularly by the central Trust team, and all staff must abide by regulations laid down by the Trust.

Access to laptops is secure, with devices being accessed using a password. Portable tablets such as iPads are 'locked down' and children and staff do not have administrator rights to download new apps or change content.

Virus protection is installed and updated regularly.

The school uses Schools Broadband for filtering

Private portable media can only access the 'guest' network and will not have access to any of the school systems. Where mobile dev ices are used by staff to access work emails, these must have access restricted through use of a password/ fingerprint or face recognition.

Email

Staff must use their school email addresses for any school related correspondence but to be aware that this is not a secure system. Passwords should be used for documents that contain sensitive information in order to comply with data regulations.

Pupils may only use approved email accounts on the school system.

Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission. This must be stressed at the point of teaching on a frequent basis.

Access in school to external personal email accounts may be blocked at the discretion of the Headteacher or Trust.

The forwarding of chain letters is not permitted.

School website

The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information is not be published.

Email addresses are generally not published, to avoid spam harvesting. Contact forms are used directly from the website, and each class has their own email address for parents/ carers from that class to use.

The Headteacher takes overall editorial responsibility and ensure that content is accurate and appropriate, along with the Trust marketing officer.

The website complies with the school's guidelines for publications including respect for intellectual property rights and copyright.

Publishing staff and pupil's images and work

Photographs that include pupils are selected carefully and do not enable individual pupils to be clearly identified by name. Permission is sought from parents and carers regarding their wishes in respect of use of photographs.

Pupils' full names will not be used anywhere on the website, particularly in association with photographs unless with specific permission (e.g. where news is within the local community and parents have authorised this).

Parents or carers are asked to notify the school, in writing, if they give permission for the school to use their child's photograph in school publications (which includes the school website).

Images of staff are not published without consent from that member of staff.

Pupils do not upload photographs or pictures of themselves or their peers to any platform in school.

Social networking and personal publishing

Social networking sites and news groups are blocked unless a specific use is approved.

Pupils are advised not to, and educated about the risks of, signing up to any social networking site that is not age appropriate, eg. Facebook

Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline telephone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.

Pupils are advised not to place personal photos on any social network space. Advice is given regarding background detail in a photograph which could identify a pupil or his/her location eg: house number, street name, school or shopping centre.

Staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of any images, along with the notion of consent.

Pupils are advised and educated about security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students are encouraged to invite known friends only and deny access to others.

Pupils are advised not to publish specific and detailed private thoughts.

The School is aware that bullying can take place through online activity, in particular social networking, especially when a space has been setup without a password and others are invited to see the bully's comments.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and General Data Protection Regulations 2018.

The school ensures that it holds the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

Staff ensure that they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

Staff use personal data only on secure password protected computers and other devices ensuring they are properly logged off at the end of any session in which they are using personal data

Authorising Internet access

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

Parents of all children are provided updates via the Newsletter of how to keep children safe online, such as advice from the Vodafone website.

Assessing risks

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school takes 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 Headteacher will ensure that the Online Safety procedures are implemented and compliance with the policy monitored.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks are reviewed regularly.

Introducing online safety to pupils

Pupils are informed that Internet use is monitored.

Online access is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. Online safety education is broad and relevant with progression related to the age and development of pupils. This is influenced by the 'Learn Together' framework.

A planned online safety curriculum is provided as part of the curriculum but, as detailed above, is revisited regularly across the whole curriculum.

Online safety messages and procedures are reinforced through assemblies, anti-bullying work and safety week.

Technical infrastructure/equipment, filtering and monitoring

All equipment is formatted for school use by our IT provider, Soltech.

Access is restricted to the role a member of staff performs in the school.

All devices are password protected, with double authentication for email systems.

Servers, wireless systems and cabling are securely located and physical access is restricted

Users have clearly defined access rights to the school's technical systems and devices

There is a 'guest' system in place for temporary users of the school network

Any material that the school believes is illegal is reported to appropriate agencies such as :

- Internet Watch Foundation (IWF) : www.iwf.org.uk or
  Child Exploitation and Online Protection Centre (CEOP) : www.ceop.police.uk o If appropriate, the Local Authority Designated Officer for Safeguarding (LADO)