FLEECEFIELD PRIMARY SCHOOL

E - Safety Policy

Last reviewed: Spring 2022

The Fleecefield e-Safety Policy is intended to cover the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity.

The policy highlights the need to educate children and young people about the benefits and risks of using new technologies both in and away from school.

It also provides safeguards and guidance for staff, pupils and visitors in their online experiences.

Fleecefield's e-safety policy will operate in conjunction with others including policies for Behaviour, Bullying, Curriculum, Data Protection, Child Protection, Health and Safety plus any Home-School Agreement.

Learning and Teaching

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.

The use of the Internet is a part of the statutory curriculum and a necessary tool for staff and pupils.

The role of the Internet to enhance learning

The school Internet access will be designed expressly for pupil use and will include 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 use digital technology to work collaboratively.

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 will be taught the Importance of cross-checking information before accepting its accuracy.

Pupils will be taught clear strategies on how to report unpleasant content.

Managing Internet Access

Information system security

School ICT systems security is reviewed regularly.

Virus protection is updated regularly.

Any guidance on security strategies issued by the Local Authority or through IT technical service will be considered and acted on.

E-mail

Our children do not use school emails. We only contact parents via email and children have access to class email addresses. Children can only communicate using the Google classroom platform on an open stream that is regularly checked by staff.

Published content and the school web site

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office. (office@fleecefield.enfield.sch.uk)

The Headteacher 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 so that their image cannot be misused, such as considering using group photographs rather than full-face photos of individual children.

Pupils full names will not be used anywhere on the school website or other on-line space, particularly in association with photographs.

Written permission from parents or carers is routinely obtained on admission, including mid-term admissions. Parents/ carers are asked to state/write their objection to the use of photographs of pupils for any school publication.

Social networking and personal publishing

The school will control access to social networking sites, and educate pupils in their safe use.

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

News groups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. This would include surnames, addresses, phone

numbers, school and specifics of clubs attended. A nickname is advisable instead of the pupil's real name.

Managing filtering

The school will work with the Technical Support Service, Local Authority and London Grid for Learning (LGfL) to ensure systems to protect pupil are monitored and reviewed.

If staff or pupils come across unsuitable on-line materials, the site must be reported to the Headteacher or Deputy Head (Curriculum).

Regular checks will be made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Staff should be aware that despite the best efforts of the school, those wishing to access children through the internet can be cunning and innovative in their attempts to break through filtering system and so staff should be vigilant in monitoring the sites used by children in their care.

Managing videoconferencing through Google Classroom

- Children can only access video conferencing using school domains, through the whole school platform (Google classroom).
- The video conferencing tool is only accessible to children if and when a member of staff has accessed and enabled the call.
- Staff will record conference calls and recordings are saved on the system
- When needed, members of staff conduct video calls with children in the presence of their parents; with groups of children or in the presence of another member of staff. These calls are planned for and timetabled accordingly
- Conference calls using the whole school platform can only be accessed by members of the organisation or if permission has been granted by a member of the organisation
- Any issues that arise from video conferencing are recorded and dealt with in line with the relevant policies

Managing emerging technologies

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

The school acknowledges the health concerns around use of mobile phones by children and prolonged sessions looking at computer screens.

Staff should be aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile phones will not be used during lessons or formal school time. The school recognises that for staff, in some very exceptional cases, mobile phones may need to be used to receive incoming calls. In these circumstances permission must be obtained from the Headteacher and phones kept on silent or vibrate. Also there may be some very exceptional cases where pupils feel they need access to their mobile phones (e.g. Young Carers), the school will look at each case individually and attempt to set up a system to remove the need for reliance and anxiety around the need for access to a mobile phone.

Mobile phones brought into school by children who are not covered by the exception above should be sent to the school office for safe keeping.

The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

The use by pupils of cameras in mobile phones will be kept under review.

Games machines including the Sony Play station, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

Staff are responsible for collecting the school mobile phone from the school office to take on school trips and home visits.

The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

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

Under the Data Protection Act 2018 parents have been given:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Information about General Data Protection Regulations (GDPR) is published on our website, as well as the contact details of the Data Protection Officer (DPO) if further information is required.

Policy Decisions

Authorising Internet access

All staff must read and sign the" Staff Code of Conduct for ICT" before using any school ICT resource The code of conduct acknowledges an awareness and understanding of the e-safety policy and 'Think then Click' rules.

The Code of Conduct can be found on CPOMS.

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

Any person not directly employed by the school must be under the responsibility of member of staff who has signed the "Staff Code of Conduct for ICT" before being allowed to access the internet from the school site.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school and staff will be vigilant but cannot accept liability for any material accessed, or any consequences of Internet access.

Complaints of Internet misuse will be dealt with by the Deputy Head (Curriculum).

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.

Parents of children involved in any misuse of the Internet will be informed.

Community use of the Internet

The school expects any community use of the school systems to adopt this e-safety policy.

Communications Policy

Introducing the e-safety policy to pupils

E- Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

Children have regular e-safety lessons to ensure that they are confident on e-safety topics

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

Staff and the e -Safety policy

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

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

Parents and carers attention will be drawn to the School e-Safety Policy.

Advice for parents received from UK Safer Internet Centre around new Apps and games is shared with parents via e-mail, the school website and school Twitter account.

Meetings for parents are held periodically to help keep them up to date with new developments.