FLEET INFANT SCHOOL
Velmead Road, Fleet, Hampshire GU52 7LQ

Telephone: 01252 613582

E-mail: info@fleet.hants.sch.uk

Policy: Online Safety Policy

Ratified by the Governing Body:

Reviewed: April 2025

Next Review Date: April 2027

Aims

The need for an online safety policy arises from the ever-changing technological world in which we live. It is essential that we educate our children about, and protect them from, any potential risks that may be posed by digital resources, including all electronic devices with imaging and sharing capabilities, not just mobile phones and cameras.

The aim of this policy is to proactively identify potential risks and identify processes for dealing with these risks, whilst recognising the statutory requirements of the National Curriculum.

1.1 Writing and reviewing the online safety policy

- The school has a Designated Safeguarding Lead and Deputies who will address any online safety issues.
- Our Online Safety Policy has been written by the school, building on Hampshire guidance. It has been agreed by senior management and approved by governors.

1.2 Teaching and Learning

1.2.1 Why the Internet and digital communications are important

- 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 statutory curriculum and a necessary tool for staff and pupils.

1.2.2 Internet use will 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 may be shown how to publish and present information to a wider audience.

• Online safety will be reinforced across the curriculum when children use the internet to enhance their learning.

• A planned online safety curriculum will be provided as part of the Computing/PDL curriculum.

• Key online safety messages will be reinforced through weekly computing lessons, biannual online safety days and termly assemblies.

• Support and promote children's mental wellbeing through controlling the content they see, ensuring interactions are suitable, and managing the amount of time spent online.

1.2.3 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.

1.3 Managing Internet Access

1.3.1 Information system security is overseen by Agile including regular review of:

• System security and filtering

• Virus protection

1.3.2 E-mail

• Pupils do not have email accounts at Fleet Infant School.

• The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.

• The school email service may only be used to communicate with others when in school or on the school system by remote access.

• Any communication using the email service must be professional in tone and content.

1.3.3 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.

• The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 Publishing pupils' images and work

• When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

• Permission is obtained from parents/carers, through the Agile system, on how the school may use, publish or display photographs of pupils. This is obtained when their child joins the school and this permission can be updated at any time during their time at Fleet Infant School. Images can only be published with the appropriate permission.

• Photographs that include pupils will be selected in accordance with the above point, so that as far as possible, individual pupils cannot be identified. Staff will consider using group photographs rather than full-face photos of individual children when appropriate.

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

• Pupil image file names will not refer to the pupil by name.

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

1.3.5 Social networking and personal publishing

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

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

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

1.3.6 Managing filtering

• Internet access is filtered for all users.

• The school will work with Agile to ensure systems to protect pupils are reviewed and improved.

• If staff or pupils come across unsuitable on-line materials, the site must be reported to the Headteacher or IT Technician.

1.3.7 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.

• All staff should note 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.

• Use of mobile phones to send abusive text messages or files by Bluetooth or any other means is forbidden.

• The senior leadership team should note that various gaming devices have wireless Internet access that will breach school filtering systems.

• Staff should be aware that contact with pupils' families is not permitted on personal devices. During school trips procedure is to contact the school first. Use of personal devices is also forbidden when taking images of children.

1.3.8 Protecting personal data

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

• The school has a data protection policy in place.

• Staff will be responsible for the security of their username and passwords.

• In cases where mobile phones must be used for communication between staff and volunteer helpers (i.e. when on an off-site visit), all details of personal mobile phone numbers collected for the trip will be destroyed on return to school.

1.4 Policy Decisions

1.4.1 Authorising Internet access

• All staff must be aware of the school's Internet Access policy before any use of the internet by staff takes place.

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

• Access to the Internet by pupils will be by adult demonstration with directly supervised access to specific, approved on-line materials.

• Any person not directly employed by the school (voluntary helpers, visitors and students) will be made aware of the school's Online Safety and Acceptable Use Policy before being allowed to access the internet from the school site.

1.4.2 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. **Neither the school nor Agile can accept liability for any material accessed, or any consequences of Internet access.**

1.4.3 Handling online 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 complaint's procedure.

• Pupils and parents will be informed of consequences for pupils misusing the Internet.

1.5 Communications Policy

1.5.1 Introducing the online safety policy to pupils

• Fleet Infant School uses the CEOP four top tips for online safety and these are shared with pupils and staff. Pupils will be taught these and these will be reinforced throughout the academic year. The four tips are displayed clearly around the school, especially where the use of ICT is more prevalent. The 'top tips' are detailed below.

Be nice to people online

People online might not be who they say they are

Do not share private information online

If you are worried – tell an adult

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

• A programme of training in Online Safety will be developed and delivered within lesson time and through termly assemblies and online safety days every other year.

• Online Safety training will be embedded within the Computing and PDL scheme of work.

1.5.2 Staff and the Online Safety policy

• All staff will be given the School Online Safety Policy and its importance explained.

• Staff will act as good role models in their use of digital technologies and mobile devices.

• A planned programme of formal online safety training will be provided for all staff and this will be regularly updated and reinforced.

• All new staff members will be given online safety training as part of their induction programme. Ensuring that they fully understand the online safety and acceptable use policy documents.

• Governors with particular responsibilities for technology/health and safety/online safety and safeguarding will attend the online safety day staff meeting.

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

• Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

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

1.5.3 Enlisting parents' and carers' support

• Parents and carers attention will be drawn to the School Online Safety Policy in newsletters and on the school web site. They will also be made aware of the relevant Acceptable Use Policy and will have to read, sign and understand their responsibilities before being allowed access in school.

• The school will ask all new parents to agree to the parent /pupil agreement when they register their child with the school and all parents and pupils will be asked to sign and understand the Acceptable Use Policies before being allowed home access to Purple Mash and Education City.

• A planned biannual online safety day will include a talk for parents to update them on current online safety issues and advise them on how to keep their children safe when accessing the internet at home.

1.6 Cyberbullying and misuse of ICT resources

• Cyberbullying is the use of ICT to deliberately upset someone else. Like other forms of bullying, it is not tolerated in school.

• The school may use disciplinary measures as a sanction against any forms of cyber-bullying or misuse of ICT resources. Pupils, parents and staff should be aware that any threatening or intimidating behaviour can be reported to the Police. (Refer to Acceptable Use Policies for guidance on misuse of ICT resources)

• Any digital evidence of cyber-bullying must be retained when incidents occur.

• Incidents of cyber-bullying should be reported to the leadership team.