



Online-Safety Policy

Revised: September 2022

Introduction

E-Safety is taught as part of every Computing lesson.

Online-Safety encompasses Internet technologies and electronic communications such as mobile phones, tablets, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's Online-Safety policy should operate in conjunction with other policies including those for pupil Behaviour and Anti-Bullying.

End to End Online-Safety

Online-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of Online-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of monitoring and filtering systems.

1.0 School Online-Safety policy

1.1 Writing and reviewing the Online-Safety policy

The Online-Safety Policy relates to other policies including those for Computing curriculum and for Safeguarding.

- Online-Safety is the responsibility of the ICT technician and the specific curriculum team. They work in close co-operation with the headteacher. The headteacher is one of the school's Designated Safeguarding Officers.
- Our Online-Safety Policy has been written by the Computing team. It has been agreed by the staff and governors.
- Online-Safety issues are included in the child protection and ICT policies.

1.2 Teaching and learning

1.2.1 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 students 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.

1.2.3 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 (see appendix 2) and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school ICT technician (123ICT)
- Staff should ensure that the use of Internet derived materials by staff and by 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.

1.3 Managing Internet Access

1.3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses broadband with its firewall and filters.
- School employees physical monitoring of internet used by pupils.

1.3.2 Use of E-mail (where applicable)

- Pupils may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- 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.
- Whilst we recognise that some members of staff who live and work within our local community and have friendships with parents as a result of this, any work-related correspondence should be undertaken through school email addresses and not through personal email or phone numbers. (See also 1.3.5)

- Parents communication should go through the office, SEN or headteacher and not directly to and from the teachers.

1.3.3 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 pupil's personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 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.

1.3.5 Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- 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 phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.
- Contact between staff members and pupils and parents on social networking sites is deemed inappropriate. (See also 1.3.2)

1.3.6 Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the ICT technician.
- The ICT technician will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.7 Managing iPads

- The ICT technician will keep the operating system and apps updated and monitor their use regularly.
- Internet access will be filtered through installed SurfProtect, which is monitored and controlled by the ICT technician.
- Staff should guide pupils in using apps and Internet sites that will support the learning outcomes planned for the pupils' age and maturity.

- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the ICT technician.

1.3.8 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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff have access to a school phone where contact with pupils or parents is required. Staff may not use personal mobile phones to contact parents except on an offsite visit, where this is deemed necessary, and access to a school phone is not possible.

1.3.9 Protecting personal data

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

1.4 Policy Decisions

1.4.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff, including Teaching Assistants must read and sign the schools acceptable user policy before using any school ICT resource.
- Only school electrical equipment (including laptops and mobile devices) will be permitted to be used in school, and personal equipment will not be authorised to be used to access the school internet or wireless access points.
- At FS/Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a permission form agreeing to comply with the school's parental acceptable user policy.
- Pupils from KS1 and KS2 will sign an acceptable user policy.

1.4.2 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 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 headteacher and governors will ensure that the Online-Safety Policy is implemented and compliance with the policy monitored.

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 head teacher.

- Complaints of a Safeguarding nature must be dealt with in accordance with school Safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Non-compliance of pupils acceptable user policy may result in:
 - discussion with class teacher / headteacher;
 - informing parents or carers;
 - removal of Internet or computer access for a period.

1.4.4 Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

1.5 Communications Policy

1.5.1 Introducing the Online-Safety policy to pupils

- Rules for Internet access will be posted in all networked rooms and on mobile ICT trolleys.
- Pupils will be informed that Internet use will be monitored.
- Advice on Online-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.

1.5.2 Staff and the Online-Safety policy

- All staff will be given the School Online-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.

1.5.3 Enlisting parents' / carers' support

- Parents' / carers' attention will be drawn to the School Online-Safety Policy in newsletters and via the Online-Safety page on the school website.

King's Meadow School

Key Stage 1 Acceptable Use Policy

- I will keep my password private
- I understand what information is personal and not to share it when I am using the computer
- I will look after all the school ICT equipment and use it properly
- I will always ask before downloading from the internet or using material I have brought into school because I understand the risks from virus infections
- I will only take a photograph or video of someone if they say it is alright
- All of the messages I send will be polite
- I will not send messages which upset other people
- I will tell an adult if I see anything which upsets me
- I will not talk to people I do not know when I'm using the internet
- I understand that the school may check my use of ICT and talk to my parent or carer if they are worried about my Online-Safety
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a period of time, even if it was done outside school

Pupil name.....

Signed.....

Date.....

King's Meadow School
KS2 Acceptable Use Policy

- I will only use the school ICT equipment for purposes I have agreed with a member of staff
- I will only go onto websites that I have been told to
- I will keep my passwords and logins private
- I will not interfere with anyone else's passwords, logins settings or files on the computer
- I will always seek permission before downloading material from the internet or using material I have brought into school because I understand the risks from virus infections
- I know I need permission to take someone's photograph or video them
- I will not send or forward messages or create material which is deliberately intended to cause upset to other people
- I will inform an adult if I see or receive any unpleasant material or messages
- I know I must take care about giving away my personal information and making contact with people I do not know using the internet
- I understand that the school may check my use of ICT and contact my parent/career if they are concerned about my Online-Safety
- I understand that if I do not follow these rules I may not be allowed to use the school computers or access the internet for a period of time and that this may apply even if the activity was done outside school.

Pupil name.....

Signed.....

Date.....

Parent / Carer Acceptable User Policy

King's Meadow School

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of Online-Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / pupils* will have good access to IT and computing to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

As the parent / carer of the above *students / pupils*, I give permission for my son / daughter to have access to the internet and to IT and computing systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, Online-Safety education to help them understand the importance of safe use of IT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT and Computing systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the IT and Computing systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's Online-Safety.

Online-Safety Audit

This quick audit will help the senior leadership team (SLT) assess whether the basics of Online-Safety are in place to support a range of activities that might include those detailed within the Computing curriculum policy.

The school has an Online-Safety Policy.	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff.	Y/N
And for parents.	Y/N
The Designated Safeguarding Coordinator is	
The Online-Safety Coordinator is	
How is Online-Safety training provided?	
All staff sign an Acceptable IT Code of Safe Practice.	Y/N
Parents sign and return an agreement that their child will comply with the school Code of Safe Practice statement.	Y/N
Rules for Responsible Use have been set for pupils.	Y/N
These Rules are displayed in all rooms with computers	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	Y/N
The school filtering policy has been approved by SLT.	Y/N
An IT security audit has been initiated by SLT, possibly using external expertise.	Y/N
School personal data is collected, stored and used according to the principles of the Data Protection Act	Y/N
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SLT.	Y/N
Have these staff attended training on the filtering and monitoring systems?	Y/N