

KPJS

E- Safety Policy



R Thomas 2021

The school e-Safety Policy covers 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 rules to guide staff, pupils and visitors in their online experiences. The school's e-safety policy operates in conjunction with other school policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection, Safeguarding Children and Security plus any Home-School Agreement.

The Computing coordinator will take the responsibility of coordinating e-safety and report to the head teacher.

Teaching and learning

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.

Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and will include filtering, provided by LGFL, 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 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 how to report unpleasant Internet content
- E Safety is embedded into curriculum lessons via CEOP materials, but also through regular assemblies, parent workshops and letters or other electronic communications

Managing Internet Access

Information system security

- The School ICT systems security will be reviewed regularly by the Computing coordinator and Beebug (our network providers).
- Virus protection will be updated regularly.

- Security strategies will be discussed with the Local Authority and Beebug.

E-mail and Communications

- Pupils Gmail, Hangout and Google Meet have been switched off. Only staff can generate a Google Meet. Children need to be accepted into a Google Meet and can be rejected or deleted for misconduct.

Published content and the school web site

- Staff or pupil personal contact information will not be published.
- Any online content will adhere the school's Social Media policy

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. The school will use group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, 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 or Social Media.
- Work can only be published with the permission of the pupil and parents/carers.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use, especially when using collaborative documents and Google Classroom.
- Newsgroups 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.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Managing filtering

- The school will work with LGFL and Beebug 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 e-Safety Coordinator.
- The Computing coordinator and Beebug will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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 are not permitted in school; technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- The use by pupils of cameras in mobile phones are not allowed.
- The appropriate use of Learning Platforms will be discussed and reviewed 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 and GDPR

Policy Decisions

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 LGFL can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the e-safety coordinator or Safeguarding team.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and an 'acceptable use' form to sign.

Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.

Appendix 1: Useful resources

www.safenetwork.org.uk/Safety-Online

www.thinkuknow.co.uk/

www.kent.gov.uk/childrens_social_services/.../e-safety.aspx

www.bbc.co.uk/cbbc/topics/stay-safe

www.ceop.police.uk/

KPJS Parent Internet and Email Agreement

Parent / guardian name:.....

Pupil name:

Pupil's class:

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, school Email and other Computing facilities at school.

I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible Computing use, outlined in the e-safety policy. I also understand that my son/daughter may be informed, if the rules have to be changed during the year. I know that the latest copy of the e-safety policy is available from the school office or on our website <http://www.kpjs.harrow.sch.uk/> and that further advice about safe use of the Internet can be found at <https://www.thinkuknow.co.uk/>

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

The school cannot accept responsibility for loss or damage to personal devices. It is not permitted for pupils to use mobile phones during the school day. Phones should not be brought into school unless there is a genuine reason for doing so and then should be handed to the teacher at registration to return at the end of the school day. Other devices should not be brought into school unless the school has given permission.

Parent's signature:.....

Date:.....

KPJS Internet and Email Agreement

Student Agreement

Using the Internet and emailing people is one way to learn at school. It is very important to be responsible and act with Integrity when using the Internet. I agree to act responsibly at all times.

When using the Internet at Kenmore Park Junior School I will:

- only work on the web for purposes specified by my teacher.
- not go looking for rude or offensive sites.
- not give out personal information such as my surname, address, telephone number, parents' work address / telephone number.
- never send a person my picture without first checking with my teacher.
- always have my teacher's permission before sending e-mail.
- compose e-mail messages using only language I understand is acceptable in my school.
- not respond to any messages that are unpleasant or that make me feel uncomfortable in any way. It is not my fault if I get a message like that. If I do receive such a message, I will inform my teacher immediately.
- not use the Internet / e-mail to call other people names, spread rumours or frighten or annoy other people. I will follow the school value of Respect with the language that I use.
- if I use my Kenmore email address at home, I will follow the same rules. I know that emails can be traced back and there will be serious consequences if I send any email / attachment that causes offense.
- I understand that we will only be able to use a 'video' link in school, not at home.
- I will not bring digital devices to school unless permission is given by the school.
- I will use my school Gsuite account only for school use as directed by my teacher. Any inappropriate actions can be traced and appropriate sanctions imposed. . I will always sign out after every use.

I understand that breaches of the rules will see me lose my Internet access rights for a period of time determined by the school.

Any misuse, bullying or use of offensive language is against school rules and there will be serious consequences.

Student Name _____

Student Signature _____

Date _____

Class _____