Online Safety Policy

Rudyard Kipling Primary School

Autumn 2024
Review Autumn 2026

RUDYARD KIPLING PRIMARY AND NURSERY SCHOOL
Rudyard Kipling School Online Safety Policy

Writing and reviewing the Online Safety policy
The Online Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The school will appoint an Online Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.
- Our Online Safety Policy has been written by the school, building on government guidance.
- This policy will be reviewed annually.

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 children 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 children.

Enhancing Learning through Internet use

- The school Internet access will be designed expressly for children's use and will include filtering appropriate to the age of children.
- Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Children will be shown how to publish and present information to a wider audience.

Children will be taught how to evaluate Internet content

- The school will ensure that the use of internet-derived materials by staff and children complies with copyright law.
- Children will be taught the importance of cross-checking information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail

- Children may only use approved e-mail accounts on the school system. They will only be able to email other children within school with '@rkps.me' email addresses. Policies will ensure that children will not receive emails from external bodies.
- Children must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, children must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened.

Published content and the school web site

- Staff or child personal contact information will not be published. The contact details given online will be the school office.
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing child's images and work

- Photographs that include children will be selected carefully so that individual children cannot be identified or their image misused. The use of group photographs rather than full-face photos of individual children will be used wherever possible.
- Children's full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website or on other online spaces. Specific permission will be sought for publication of photographs on the school social media feed (Twitter - @RudyardSchool)
- Work can only be published with the permission parents/carers.
- Child image file names will not refer to the child by name.
- Parents will be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate children in their safe use. We will use a recognised scheme to teach Online Safety and digital resilience. Currenty we are using the eAware online portal and schemes of work.
- Children will be taught never to give out personal details of any kind which may identify them, their friends or their location.
- Children and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged children.
- Children will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school will work with Brighton & Hove City Council, to ensure systems to protect children are reviewed and improved.
- If staff or children come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Children will not be able to individually make or answer videoconference calls.
- Videoconferencing and webcam use will be appropriately supervised for the children's age.
- Whole class video conference calls will only be made with individuals who have been appropriately vetted by the senior leadership team.

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 senior leadership team 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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. Children's mobile phones will be collected by the school office at the beginning of the school day and returned to children at the end of the day.
- While on the school grounds, children are not permitted to use their mobile phones to take photographs, access websites or interact with social media.
- The use of games machines including the Sony PlayStation, Microsoft Xbox, Nintendo Switch and others that have Internet access which may not include filtering and are not permitted.
- Staff will be issued with a school iPad to capture photographs of children and must not use their own cameras or devices for this.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018/GDPR regulations. Out data protection procedures and systems are detailed in our Data Protection policy.

Policy Decisions

Authorising Internet access

- All staff must read and sign the “ICT Usage Policy" before using any school ICT resource.
- The school will maintain a current record of all staff and children who are granted access to school ICT systems.
- Parents will be asked to sign a parent/child agreement which will include a sections on acceptable use of computers in school as well as expectations regarding the usage of social media by parents/carers/children out of school
- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources’ 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. Neither the school nor B&H city council can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by the Headteacher.
- 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.
- Children and parents will be informed of the complaints procedure (see schools complaints policy)
- Children and parents will be informed of consequences for children misusing the Internet.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communications Policy

Introducing the Online Safety policy to children

- Online Safety rules will be posted in all rooms where computers are used and discussed with children regularly.
- Children 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, based on the materials from eAware

- Online Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.
- There will be an additional focus on Online Safety through the yearly focus of ‘Safer Internet Day’ (https://www.saferinternet.org.uk/).

Staff and the Online Safety policy

- All staff will be given the School Online 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 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 children.

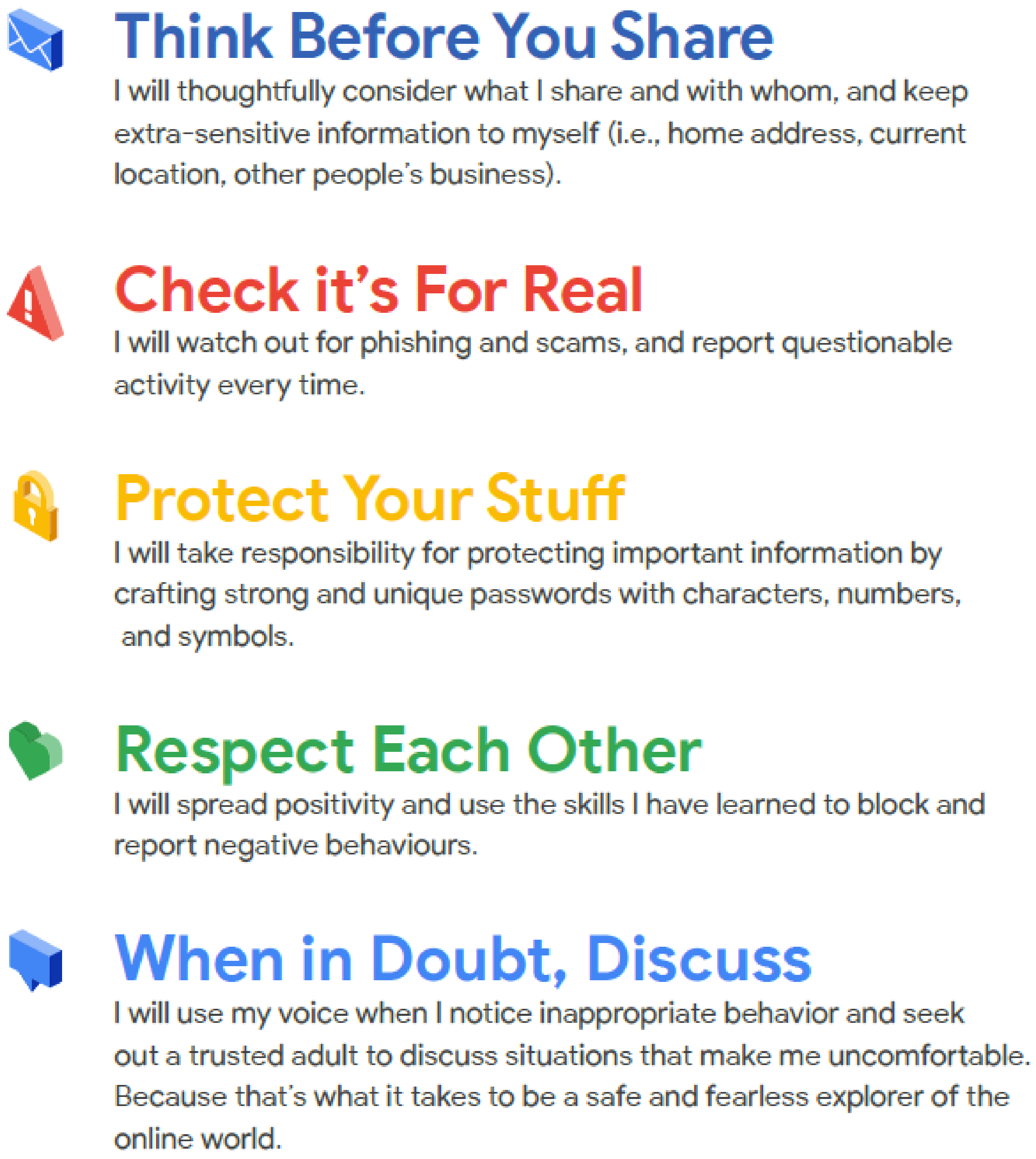
Enlisting parents’ and carers’ support

- Parents’ and carers’ attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of Online Safety resources for parents/carers.
- The school will ask all new parents to sign the parent/child agreement when they register their child with the school.

Review Date: Autumn 2026

Online Safety rules for children (from Google's 'Be Internet Legends' scheme).

The Internet is a brilliant place to explore and learn but needs to be used carefully and responsibly. When we use computers at home or at school we agree to follow these important rules:



Think Before You Share

I will thoughtfully consider what I share and with whom, and keep extra-sensitive information to myself (i.e., home address, current location, other people's business).

Check it's For Real

I will watch out for phishing and scams, and report questionable activity every time.

Protect Your Stuff

I will take responsibility for protecting important information by crafting strong and unique passwords with characters, numbers, and symbols.

Respect Each Other

I will spread positivity and use the skills I have learned to block and report negative behaviours.

When in Doubt, Discuss

I will use my voice when I notice inappropriate behavior and seek out a trusted adult to discuss situations that make me uncomfortable. Because that's what it takes to be a safe and fearless explorer of the online world.

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Online Safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will ensure that my information systems use will always be compatible with my professional role.

- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.

- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.

- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.

- I will not install any software or hardware without permission.

- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the school Online Safety Coordinator or the Designated Child Protection Coordinator.

- I will ensure that any electronic communications with children are compatible with my professional role.

- I will promote Online Safety with children in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: ____

Date: ____

Please print name: ___________________________________