



Online Safety Policy

Date Policy was formally adopted	November 2019
Review Date	November 2020
Chair's Name	
Chair's Signature	

Core Values

Respect

Enjoyment

Care

Confidence

Challenge



Rodings Primary School

Online Safety Policy

Writing and Reviewing the Online Safety Policy

The Online safety policy is part of the school's wider role in Safeguarding and relates to other policies including those for Computing, Anti-bullying and Child Protection.

- The Computing subject leader will ensure that the Online Safety policy is kept up to date, working with the Designated Safeguarding Lead.
- The policy will be reviewed yearly because of the forever changing developments in technology.

Teaching and learning

Why the internet and digital communications are important

- The internet is an essential element in the 21st century life of education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of the 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 will be designed expressly for pupils use and will include filtering appropriate to the age of the pupils. This is provided by Broadband provider.
- Children will be taught what internet use is acceptable and what is not and given clear objectives for internet use
- The curriculum has been designed so that each year group has a dedicated online safety module per year.
- Children will be given a reminder about appropriate use every time they use the internet.
- Children will be educated in the effective use of internet research, including the skills of knowledge location, retrieval and evaluation.
- Children will be shown how to publish and present information to a wider audience.

Pupils 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.
- Children will be taught how to report unsuitable internet content e.g. using CEOP Report Abuse icon or red flag icons.

Managing Internet Access

Information system security

- School computing system will be reviewed regularly
- Virus protection will be updated regularly.
- Security strategies will be discussed with local authority or IT maintenance provider, IT provider.

E-mail

- Children may only use approved email accounts on the school system.
- Children must immediately tell a teacher if they receive an offensive email.
- In email communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming emails should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how emails from pupils to external bodies are presented and controlled.
- The forwarding of chain letters are not permitted.

Published content and the school website

- Staff or children's personal contact information will not be published. The contact details given online should be the school office or part of a school email system.
- The head teacher will take overall editorial responsibility to ensure that content is accurate and appropriate.

Publishing pupils' images and work.

- GDPR legislation makes it very clear how photographs should be used. On entry to school Parents complete a photograph permission slip that clearly identifies what use they are giving permission for.
- Photographs that include children will be selected carefully so that their image is not misused. Consider using group photographs rather than full face photos of individual children.
- Children's full names will not be used anywhere on a school web site or other on-line space, particularly in association with photographs.
- Children's 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.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate children in their safe use.
- Forums, blogs, vlogging will be blocked unless a specific use and safe site is identified and approved.
- Children will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Ideally pupils would use only moderated social networking sites e.g. Class Dojo
- Children and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary age pupils.

- Children will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school will work with Broadband provider and IT provider to ensure systems to protect pupils are reviewed and improved.
- If staff or children come across unsuitable online materials, the site must be reported to the Computing subject leader or a member of the SLT.
- The Computing subject leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing and webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Children must ask permission from the supervising teacher before making or answering a video conference call.
- Videoconferencing and webcam use will be appropriately supervised for the child's age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefits 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 materials 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.
- The use of cameras on mobile phones will not be permitted.
- Games machines including the Sony PlayStation, 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.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the GDPR legislation.

Authorising internet access

- All staff must read and sign the 'Staff Code of Conduct' and 'Acceptable use' policy before using any school computing resources.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- At Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.
- Parents consent for children to use the internet is gained through the on entry pack of permissions.

- Any person not directly employed by the school and using technology unsupervised will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.
- A guest account will be set up for visitors e.g. supply teachers, work experience students.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate materials. 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 Broadband provider can accept liability for any material accessed, or any consequences of internet access.
- The school should audit IT 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 or the Deputy Headteacher.
- Online safety incidents will be recorded on MyConcern which all staff have access to.
- 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 and the revised SET procedures (2019).
- Pupils and parents will be informed of the complaints procedure (see school's complaints policy). This is available in the school handbook.
- Children and parents will be informed of consequences for pupils misusing the internet through the Home School Agreement.
- Discussions will be held with the local Police Officers to establish procedures for handling potentially illegal issues or referred to the Children and Families Hub.

Community use of the internet

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

Communications Policy

Introducing the online safety policy to pupils

- Online safety rules will be posted in every classroom and near to where computers are stored and discussed with children regularly.
- Children will be informed that networked and internet use will be monitored and appropriately followed up.
- A programme of training in online safety will be developed.
- Online safety training will be embedded within the Computing scheme of work and/or the Personal Social and Health Education (PSHE) curriculum.

Staff and the online safety policy

- All staff will have access to the school's 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 IT use will be supervised by the SLT and work to clear procedures for reporting issues.
- 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 online safety policy in the school newsletter, the school prospectus and on the school website.
- The school will maintain a list of online safety resources for parents/carers.
- The school will ask all new parents to sign the Home/School agreement when they register their child with the school.

Also refer to the Acceptable Use Policy (Included in the Code of Conduct policy) for staff.