



REDHILL

PREP SCHOOL & MONTESSORI NURSERY

E-SAFETY POLICY

The e-Safety Policy is part of the ICT Policy and School Development Plan and relates to other policies including those for ICT and child protection.

- The school will appoint an e-Safety Coordinator.

This will be Adrian Thomas (Head teacher)

- Our e-Safety Policy has been written and has been agreed by the senior management.
- The e-Safety Policy and its implementation will be reviewed annually.

TEACHING AND LEARNING

Why is Internet use 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 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 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.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be taught how to evaluate Internet content

The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

The evaluation of on-line materials is a part of every subject.

MANAGING INTERNET ACCESS

Pupils will be taught how to evaluate Internet content

The security of the school information systems will be reviewed regularly. Virus protection will be updated regularly.

Email

Redhill Preparatory School e-mail addresses will be used in school and access gained only by teachers entering passwords.

Email is provided for pupil use in school using purple mash. It only allows internal emailing.

Pupils must immediately tell a teacher if they receive offensive e-mail or report via purple mash report button.

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 external organisations (eg. Other schools) should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school website and blog, facebook page and twitter

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.

The Headteacher will ensure editorial content is suitable, accurate and appropriate.

Publishing pupil's images and work

Pupils' full names will not be used anywhere on the website, blog, face book in association with photographs.

Written permission from parents or carers will be obtained before images of pupils are electronically published.

Work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

The schools will block/filter access to social networking sites.

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 and / or their location.

Managing Filtering

The school will ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator so that they can be blocked in future.

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 children are not allowed to bring mobile phones to school. The sending of abusive or inappropriate text messages is forbidden.

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

POLICY DECISIONS

Authorising Internet access

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All staff must read and sign the Staff Acceptable Use Policy before using any school ICT resource.

All pupils will be asked to sign the Pupil Acceptable User Policy before using any school ICT resource.

Parents will be asked to sign an Acceptable User Policy for pupil use.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

Handling e-safety concerns

E Cadets report e safety concerns to the ICT coordinator

E Cadets update the pupil website under supervision. No access to passwords.

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the E-safety Coordinator.

The school has a bully button on the school website

COMMUNICATIONS POLICY

Introducing the e-safety policy to pupils

Pupils will be informed that network and Internet use will be monitored.

Instruction in responsible and safe use should precede Internet access

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its application and importance explained.

Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

Enlisting parents' support

Parents' attention will be drawn to the school's e-Safety Policy on the school website.

Internet issues will be handled sensitively, and parents will be advised accordingly.

Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

A bulletin or email of guidelines about any arising issues will support parents.

Signed by E-safety Co-ordinator

Head
Teacher.....

Date.....Review Date.....

Document Checks			
Document	E-Safety	Reviewed by	SMT
Category	Policy	Date	Autumn 2021
Date Issued	Autumn 2012	Next Review	Autumn 2022
Approved by Staff	Autumn 2012	Monitored by	AT