Safe Use of the Internet Policy

Prepared for:

Redwood and Parkview Primary School

Date: November 2020

Review: March 2023

Author: Tessa Duffield

Policy review dates and changes

Review date	By whom	Summary of changes made	Date ratified by governors/trustees	Date implemented
March 2024	Marie Jarvis	Removal of reference to remote learning during Covid. Additions to '**How will the school ensure Internet access is safe?**' section only. **Addition to 'How will the security of school ICT systems be maintained?' section:** Training for school staff on cyber security and data privacy completed every 3 years.		

Safe Use of the Internet Policy

Rationale

This document is a statement of the schools commitment to ensuring Safe Use of the Internet at Parkview and Redwood Primary Schools.

Aims

To ensure that

- *All members of the school community – children, teachers, parents and governors – are aware of the need for safe and responsible internet use*
- *The issues surrounding internet safety are discussed*
- *Internet use supports schools' educational aims*
- *LA requirements are satisfied.*

Implementation of the Policy

What is the need for Internet Access at school?

- School internet use is now an important part of teaching, learning, administration and communication
- It makes possible a wider range of information, the scope and nature of which may or may not be appropriate
- Used responsibly it can raise educational standards, support the professional work of staff and to enhance the school's management information and business administration systems.
- It is a beneficial learning tool when children have been taught to understand its value and limitations.

How can the Internet be used as a teaching and learning tool?

Teachers, parents and children should be able to develop good practice in using the Internet as a tool for teaching and learning. We believe that:-

- *Internet access will enrich and extend learning activities.*
- *On-line activities that will support the learning outcomes planned for the children's age and maturity.*
- *Children should be confident using the Internet for research, including the skills of knowledge location, retrieval and evaluation of material* found.

What are the benefits?

Benefits of internet access at Primary level include:

- *Access to world-wide educational resources including museums and art galleries*
- *Educational and cultural exchanges between children world wide*
- *Cultural, vocational, social and leisure use in libraries, clubs and at home*

- *Access to experts in many fields for children and staff*
- *Staff professional development through access to national developments*
- *Educational materials and good curriculum practice*
- *Communication with support services, professional associations and colleagues*
- *Improved access to technical support including remote management of networks*
- *Exchange of curriculum and administration data with the LA and DfE.*

How will children be taught to assess Internet content responsibly?

- Children will be taught ways to validate information before accepting that it is necessarily accurate.
- Children will be taught to acknowledge the source of information, when using Internet material for their own use.
- Children will be made aware that the writer of an email or the author of a Web page might not be the person claimed.
- Children will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

How will email be managed?

Email is an essential means of communication within education and the government is encouraging the ownership of personal email Ids for both teachers and children. Children need to use email as part of the National Curriculum.

The following rules for email use will be as followed:-

- ✓ Email must only be used in school for educational purposes.
- ✓ Children will not be allowed to access personal email from the school system.
- ✓ In coming email will be regarded as public. Received email may be examined and could, for example, be pinned to a notice board.
- ✓ Messages sent using the school domain name should be regarded in the same way as messages written on school headed paper.
- ✓ The forwarding of e-letters is not permitted.

How will publishing on the Web be managed?

As Parkview and Redwood Primary School Web sites can be accessed by anyone on the Internet, the security of staff and children is paramount. The publishing of children's names beside photographs that identify individuals will not occur.

- ✓ All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name
- ✓ The point of contact on the Web site is the school address and telephone number. Home information or individual email identities will not be published.
- ✓ Photographs must not identify individual children.

- ✓ Full names will not be used anywhere on the Web site, particularly alongside photographs.
- ✓ Parents are informed of the school policy on the use of photographs via the school prospectus. Reminders are given at school events. Parents are requested not to publish photographs on social media sites unless only their own child is featured.

How will Internet access be authorised?

- *At Foundation Stage and Key Stage 1, the majority of the access to the Internet will be by teacher or adult demonstration or via the school learning platform. However there may be situations when children have access to specific approved on-line materials.*
- *At Key Stage 2, Internet access will be granted to a whole class as part of the scheme of work, after a suitable education in responsible Internet use.*

How will the risks be assessed?

It is difficult to remove completely the risk that children might access unsuitable materials via the school system whatever safeguards are put in place.

- *Due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal*
- *Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences thereof.*
- *The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990*
- *Methods to identify, assess and minimise risks will be reviewed at the same time as the policy is reviewed.*
- *Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken.*
- *All staff are responsible for ensuring that the policy is implemented effectively.*

How will the school ensure Internet access is safe?

- The system the school will use is a blocking system operated by Mercury AVS.
- Children will be informed that internet use will be supervised and monitored. Mercury AVS will notify the Headteachers of both schools if a search has been conducted on a school device which is a cause for concern. The Headteachers of each school will investigate these alerts if they feel it is suitable and keep a log of the action taken.
- The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect children are reviewed and improved.
- Headteachers will ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice. Usually, this will be done using 'Test My Filter'. Headteachers will keep a log of these checks and record actions taken from said filter checks.
- The computing lead teacher/Headteacher will check the filters on both children's and staff accounts termly.

- In the unlikely event that staff or children discover unsuitable sites, the URL (address) and content will be reported to the Internet Service Provider via the School Business Manager and blocked through the schools computer filters.
- As most internet use in our primary schools is supervised, the risk to children is low.

How will the security of school ICT systems be maintained?

- Security strategies will be discussed with the LA and Mercury.
- The security of the whole system will be reviewed with regard to threats to security from Internet access.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Virus protection will be installed and updated regularly.
- Confidential material is received and sent by the school using the Egress password protected email system.
- Training for school staff on cyber security and data privacy completed every 3 years.

How will complaints regarding Internet use be handled?

- Prompt action will be required if a complaint is made. The facts of the case will need to be established as quickly as possible.
- Responsibility for handling incidents rests with the Head of School.
- Sanctions available include interview/counselling and, if appropriate, informing parents or carers.
- A pupil may have email, Internet or computer access denied for a period of time depending on the nature of the incident.

How will staff and children be informed?

- The E-Safety policy will be displayed on the school's website.
- Staff will undertake E-Safety training and records will be kept to ensure training is updated at regular intervals.
- E-safety posters are displayed in all classrooms.
- E-safety is taught discreetly every half term and the school takes part in Safer Internet Day during February and November.
- Children will also be taught about being safe on the internet as part of the PSHE curriculum.

Disability Equality Impact Assessment

This policy has been written with reference to and in consideration of the school's Disability Equality Scheme. Assessment will include consideration of issues identified by the involvement of disabled children, staff and parents and any information the school holds on disabled children, staff and parents.

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

This policy will be reviewed in line with the school Policy Review Cycle.

Related policies:

- Child Protection and Safeguarding Policy
- Complaints Policy
- Data Protection Policy
- Freedom of Information Publication Policy
- ICT Policy
- Positive Behaviour Policy