Nevill Road Junior School

Title	E-Safety Policy	Version
Author	Nevill Road Junior School	
Approved by	Full Governors	May 2023
Review Date		May 2026

Introduction

At Nevill Road Junior School we recognise that ICT and the use of the Internet plays an important role in children's learning. It is important that the children in our school see both the benefits and the risks of using new technologies. Our Internet Safety policy explains the need for providing safeguards and awareness for users to enable them to control their online experience.

The school's E-safety policy also operates in conjunction with other policies including those for Positive Relationships and Behaviour (incorporating Anti-Bullying, Learning and Teaching, and Data Protection and Security).

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. We have 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 uses central LA filtering services to ensure content that is accessed is appropriate to the age of pupils.
- At Nevill Road Junior School, pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. This will be completed in both Computing and PSHE lessons.
- During lessons, our children 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

- At school, we will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Through our Computing, and PSHE lessons, our pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Stockport local authority and developed with our ICT technician.

E-mail

- Our pupils only use an approved class e-mail account on the school system.
- Pupils are taught to immediately tell a teacher if they receive offensive e-mail.
- Through our specific lessons, children at Nevill Road Junior School are taught not to reveal personal details of themselves or others in e-mail communication, to open messages from unknown parties, or to arrange to meet anyone without specific permission.

Published content and the school website

- The contact details on our school website are the school address, e-mail and telephone number. Staff or pupils' personal information is **not** published.
- The head teacher takes overall editorial responsibility of the website and ensures that content is accurate and appropriate.

Publishing pupil's images and work

- Pupils' full names will not be used anywhere on the website, blog or twitter, particularly in association with photographs.
- Written permission will be sought annually from parents or carers before photographs of pupils are published on the school website/twitter.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school and LA block access to social networking sites with the exception of twitter.
- Newsgroups are blocked unless a specific use is approved by an appropriate member of staff.
- Pupils are routinely advised never to give out personal details of any kind which may identify them or their location, or to accept 'friend requests' or respond to other messages from unknown parties, and to report these where appropriate.
- Pupils are made aware of the dangers of social network spaces and how to minimise the risk
- Parents are made aware of the dangers of social network spaces and how to promote responsible use at home.

Managing filtering

- The school will work with the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Designated Safeguarding Lead and logged on CPOMS.
- Senior staff 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 for use by pupils in school.
- Staff should not use their mobile phones in the presence of pupils (see Safeguarding Policy for further details)
- Pupils and their parents accept full responsibility for any personal 'devices' which they choose to bring into school to assist them with their work.
- Staff will use a school phone where contact with pupils is required.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff must read and sign the '**STAFF E-SAFETY ACCEPTABLE USE AGREEMENT** before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Children and parents must sign the **'Responsible Use of the Internet and Computers in School' Agreement** before using any school ICT resource.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor Stockport LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.

Community use of the Internet

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

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be reminded of the E-safety rules at the beginning of each half term and regularly referred to throughout the year.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will be educated in safe internet use in the home.
- The school will inform parents about E-safety so they can use the internet safely at home.
- Parents will have the opportunity to discuss any concerns with a member of staff

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained. It will be referred to in the Staff Handbook and will therefore be discussed during induction of any new staff and each September (INSET).
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, at e-Safety events and on the school website.