Norwood Green Junior School

e-Safety Policy

Policy ratified by the GB: March 2025

Policy to be reviewed: March 2028

Writing and reviewing the e-safety policy

Norwood Green Junior School's e-Safety Policy has been written by the school, following government guidance, 'Keeping Children Safe in Education and 'UK Council for Child Internet Safety (UKCCIS). It has been agreed by senior management and approved by governors.

2 Teaching and learning

Why Internet use is important?

- The Internet is an essential element in life for education, business and social interaction. The school believes it has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school's Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught acceptable and non-acceptable Internet use and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils are taught how to evaluate Internet content

- E-Safety is taught as part of both PSHE and Computing. The School follows statutory objectives from both: 'Online Relationships' within the document 'DFE Relationships Education 2021' and the 'Primary Computing National Curriculum 2014'.
- There is a clear progression of skills from Y3-Y6.
- Every half term the series of Computing lessons starts with an E-Safety lesson. Lessons are regular and spread throughout the year rather than taught in a block. This approach ensures that E-Safety is continuously considered by pupils.
- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3 Managing Internet Access

Information system security

- School computing security are reviewed regularly.
- Virus protection is updated regularly.

E-mail

- Pupils may only use approved e-mail accounts on the school system. Currently pupils are not using emails in school. It is planned that when they do, they will do so in a safe way which does

not allow them to contact or to be contacted by anyone outside of the school community i.e. only used on a teaching basis with other pupils in their class or perhaps year group.
- Pupils are instructed to immediately tell a teacher if they receive an offensive e-mail.
- Pupils are taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Published content and the school web site

- The contact details on the Web site are the school address, school e-mail and school telephone number. Staff or pupils' personal information will not be published.
- The Headteacher takes overall editorial responsibility to ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Pupils' full names are not used anywhere on the web site.
- Parents have the right to opt out of photographs of their child or child's work being published on the school web site.
- Pupil's work is published with the permission of the pupil and parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites and other inappropriate sites.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- The school seeks guidance from the DfE and works with the IT 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 Leadership Team.

Managing emerging technologies

- Emerging technologies are examined for educational benefit and potential risks to children are discussed.
- Mobile phones will not be used during lessons by pupils and staff. The sending of abusive or inappropriate text messages is forbidden. Pupils are not allowed to have mobile phones during the school day. Parents can request that their child's phone is kept by the class teacher in a locked cupboard during school time and then issued to them at 3:30 if they walk home alone. If the teacher feels that they do not want this responsibility or feel that there is a risk of theft they are to discuss phones being kept in the office instead.
- Staff of children in the Centre for the Deaf have a school mobile to text parents from. Texts are also sent to parents from the school office, via the school's Text 2 Parents software. *See Acceptable User policy.*

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 2018.

DFE laptops lent to families

- Parents who are provided with a laptop to borrow have to sign a loan contract. This explains expectations of use: Used only by a pupil of Norwood Green Junior School for educational purposes. They are not allowed to save content on the laptop. On return of the laptop to school, devices are checked for saved content and internet searches.

4 Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Agreement'.
- At NGJS, access to the Internet is adult supervised although the adult may not be required to stay with the pupil for the entire time that they are using the internet. Consent from parents for their child to use the internet is given via the 'contact' details form.

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. The school cannot accept liability for the material accessed, or any consequences of Internet access. Nevertheless, the school will seek to protect pupils within reason in liaison with its IT provider.

Handling e-safety complaints

- Complaints of Internet misuse are dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher. *See Acceptable Use Agreement and Whistleblowing Policy.*
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. *See Safeguarding Policy.*
- Failure to comply with this policy will be investigated by a senior member of staff and could lead to disciplinary procedures.

Community use of the Internet

- When appropriate, the school will liaise with organisations (e.g. Sweethaven, Norwood Green Junior School's IT provider) to establish a common approach to e-safety.

5. Communications Policy

Introducing the e-safety policy to pupils

- E-safety is taught to pupils on a termly basis. Pupils will be informed that network and Internet use will be monitored. Specific e-safety lessons will be taught annually to all pupils.

Staff and the e-Safety policy

- All staff are made aware of the nature of e-Safety Policy and its importance through its regularity of lessons planned for as part of the computing curriculum.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. *See Acceptable Use Agreement, Conduct, Grievance and Discipline Policy.*

Enlisting parents' support

- Parents' attention will be drawn to e-Safety through a variety of means including being provided a monthly e-safety newsletter, guidance on child safety online through both the School website and annual parent curriculum meetings.

Related Policies:

Whistleblowing
Acceptable Use Agreement
Child Protection and Safeguarding
Dealing with Allegations of peer to peer abuse
Security Policy
Camera and Image Use Policy
Anti-Bullying Policy
Data Protection and Information Sharing and Confidentiality
Conduct, Discipline and Grievance Policy
Dealing with allegations Against Staff