Waverley Primary School

E – Safety Policy

Teaching and learning

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.
- 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.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work

See appendix 1 for **Teaching E-Safety Awareness across KS1 and KS2**

Management of e-mail

- Pupils may only use approved e-mail accounts in school. This system ensures privacy and data are protected.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff will operate the sharing of data and information as per guidelines. The restrictions of sharing data outside of our school and wider Trust networks will help enable we abide by data protection guidelines and General Data Protection Regulations (GDPR).

Management of published material

The contact details on the website should be the school address, e-mail and telephone number. The only staff information to be published on the school website and blogs are staff surnames and job titles. No surnames of pupils will be used on the school website, blogs or newsletters. When a photo of the child is present on the website, there will be no name provided.

E-mail addresses should be published carefully, to avoid spam harvesting.

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on the website, where a photograph is present. Only one or the other will be used.

A letter notifying Parents/Carers about the use of their child's photograph on the school website will be sent out at the start of every academic year. If parents do not wish for their child's photograph to be published electronically then they must sign the relevant form attached to the letter.

Management of social networking and personal publishing

- The school will block access to social networking sites, however, the school will educate pupils in the safe use of social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

- We are aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator.

How will emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time.
- The sending of abusive or inappropriate text messages is forbidden.
- Children with a mobile phone must hand them to the office in the morning.
- Staff will not have mobile phones on their person during lesson times.

Authorised Internet Access

- All staff must read and sign the Staff Code of Conduct agreement before using any school Computing resource.
- At Key Stage 1, access to the internet will be by adult demonstration and regular directly supervised access to specific, approved on-line materials. 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.
- Nether school nor LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- 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.

E-safety awareness

- E-safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network and internet use will be monitored.
- An e-safety assembly is delivered across the school to raise awareness and importance of safe and reasonable internet use.
- Instruction in responsible and safe use should precede Internet access.
- All staff will be given access to the school e-safety policy and its application and importance explained.
- Staff should be aware that Internet traffic is monitored and traced to the individual user.
- Discretion and professional conduct are essential.

Community and parent awareness

- Parents' attention will be drawn to the school's e-Safety Policy via pupils' work via Computing sessions/assemblies and in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This will include parent evenings with demonstrations and suggestions for safe home Internet use.
- Parents are able to contact the school office to discuss an e-safety issues or concerns.

Home Learning

- The e-safety policy also applies to Seesaw, the home learning platform. It is important for staff to follow normal school procedures and codes of conduct when using Seesaw.
- Only use school authorised accounts and learning platforms when corresponding with pupils and parents / carers.
- It is expected that staff make online behavioural expectations clear to pupils and model good practise when using technology.
- E-safety will continue to be taught via the online learning platform.
- Any concerns about online safety will be reported via CPOMS and to Senior Leadership Team as appropriate.

See appendix 2 for **Home Learning Policy**

Policy reviewed by Computing lead: January 2021
Review: January 2022