Westfields Infants School
E Safety Policy

Westfields Infant School is committed to ensuring that we are able to operate with safety and confidence whenever the internet, learning platform and any/or mobile technology is used.

E-Safety encompasses Internet technologies and electronic communications such as E-mail, mobile phones and personal publishing whilst using computers, iPads and mobile devices. It highlights the need to educate pupils, parents and staff about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff, pupils and parents.
- Sound implementation of e-safety policy in both administration and curriculum.
- Safe and secure broadband from Hampshire including the effective management of a filter.

All users must take responsibility for abiding by the appropriate guidelines in this policy.

Computers, the Internet and mobile technology are an essential part of life and have a valuable role to play in the education of our pupils. Our school has a duty to provide our pupils with quality Internet access as part of their learning experience.

All staff are expected to read and sign the 'Acceptable Use Policy' covering appropriate use of school technology

Managing internet access

Our computer network, both curriculum and admin, are supported by Harrup. The school uses filters, restricting many sites they consider inappropriate. If unsuitable sites are discovered the URL, time and date must be reported to the network administrator. Websites will be previewed and evaluated by the teacher prior to class use. Children will not be allowed to use chat rooms, instant messaging sites, social networking sites or news groups in school.

Staff and classes will have their own user names and passwords to gain access to the school network. Each individual will be responsible for accessing the network responsibly. Everyone must be aware that internet use can be monitored and traced to an individual user or class.

The school will take reasonable precautions to ensure users access only appropriate material. However, due to the international scale and linked nature of the internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. If this happens the school will inform Hampshire and the parents of any children who may have been exposed to the inappropriate material.

Neither the school or Hampshire can accept liability for the material accessed or any consequences of internet access.

School Website

The contact details on the website should be the schools address, e-mail and telephone/fax number. Staff or pupils personal details will not be published. The site will be checked regularly to ensure that the content is accurate and appropriate. Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified without the parents permission. Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Roles of individuals

1. Head teacher - The head teacher will take ultimate responsibility for internet safety issues within the school while delegating day to day responsibility to the appropriate staff. They will support the promotion of e-safety to the school and parents and ensure it's embedded across the curriculum**.**

2. Computing Subject Leader - The subject leader will develop and implement appropriate e-safety policies and procedures, with support from the Network manager and Headteacher. The subject leader will ensure that e safety is included in the school's planning.

3. Network Manager - The network manager will provide a technical infrastructure to support e-safe practices with the support of Harrup. They will take responsibility for the security of systems and data and report any technical breaches to the Headteacher and take appropriate action as advised.

4. All staff - Staff will embed e-safety education in curriculum delivery wherever possible and will maintain a professional level of conduct in their personal use of technology, both within and outside school.

5. Pupils - Pupils need to understand the risks of the internet. Children will be taught about the dangers they may encounter and what to do if they feel that they are in danger or if they are worried. Children will be taught to tell any adult if they find something strange or worrying on the internet. It will be reinforced that they are not to blame and will not get told off.

6. Parents - Parents have a key role to play in the internet safety education of their children through promoting internet safety at home. ICT offers the opportunity for children and their parents to learn together, and internet safety is an excellent topic that can encourage home-school links. Parents and carers attention will be drawn to the policy and home support through the school webpage or by enquiring at the school office

Managing emerging technologies and assessing risks

Emerging technologies will be examined for educational benefit and an unwritten risk assessment will be carried out before use in school is allowed. Mobile phones are not allowed on the school site by pupils and staff are not permitted to use these during lessons or formal school time.

Staff should be aware that technologies such as mobile phones or playstations with a wireless network could bypass school filtering systems and present a new route to undesirable material and communications.

Handling complaints
Complaints of internet misuse by staff, pupils or parents will be dealt with by the Head Teacher. Complaints of a child protection nature must be dealt with in accordance with school's safeguarding and child protection and procedures.

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

Linked policies:
Safeguarding
Child protection
Acceptable Use
Computing

Approved by Governors: Spring 2022

Review: Spring 2025