The Horsell Village School

Online Safety Policy

Introduction

At 'The Horsell Village School' we recognise that the internet and digital communications are important and that internet use can enhance learning for our children. The Internet is an essential element in 21st century life for education, business and social interaction. We have a duty to provide students with quality Internet access as part of their learning experience. In addition, Internet use is a part of the statutory curriculum and a necessary tool for staff and children.

Providing Internet Education

- Children will be educated in how to effectively use the Internet in research and be taught how to use child friendly search engines.
- Children will be taught how to begin to evaluate Internet content and to be aware of the materials they read or see.
- Children 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.
- Staff should guide children in online activities that will support learning outcomes planned for the children's age and maturity.
- Children will regularly learn about online safety across the computing and PSHE curriculum and during whole school reflections once a term.
- Children will be taught about the risks of sharing digital content online including images and videos and begin to become aware of their digital footprint.

Keeping Staff and Children Safe

- The school Internet access is provided by a BT contract and the school has a SmoothWall (local) filtering system in place appropriate to the age of the children.
- iPads are managed by the Meraki system manager for iPads and controlled by OrbitTech, our contracted technical team.
- Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Children will be taught how to report unpleasant Internet content and encouraged to follow the HVS online safety poster as displayed in every classroom and attached to every laptop and computer.
- One member of staff will have Advanced Online Safety Training (Keeping children safe online run by the NSPCC) and share regular updates with staff through annual training sessions and where necessary briefings during Wednesday meetings. This will ensure all staff are aware of the current risks involved with children's online use and also how they can personally keep themselves protected and are aware of their own digital footprints.

Responsible Use

- The school will seek to ensure that the use of Internet derived materials by staff and by children complies with copyright law.
- Email to parents is protected by a secure log in system and has restricted staff use.
- All staff must read and sign the Computing code of conduct Agreement within the Portable Computing Device and Removable Media Security Policy, before using any school computing resource.

Managing Internet Access

- School computing systems security will be reviewed regularly, using both AVG business security to provide virus protection, Malware and Phishing protection and SmoothWall to log what is being used on the internet.
- Malware and Phishing protection are all set to automatically update as updates are released.
- Filtering is customised for both staff and children.
- The school email system (RM Unify linked to Office 365) is encrypted and scans each email on receipt.
- SmoothWall logs what is used on the internet and basic reports can be produced to highlight which websites have been accessed by individual users and which search terms have been used. Incoming e-mail should be

treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

Published content and the school website
- The contact details on the website should be the school address, school e-mail and telephone number. Staff or children personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing children's images and work

- Photographs that include children will be selected carefully, will not give any child's name.
- Children' names will not be used on the website, including in children' work and videos particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website or any other publication.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic devices.
- Children must not reveal personal details of themselves or others in any online communication, or arrange to meet anyone without specific permission.
- Staff will be aware of the risks involved in sharing images and photos online and will select images carefully.

Managing filtering
- The school will work in partnership with BT and the Swan Trust to ensure systems to protect children are reviewed and improved.
- If staff or children come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator.
- Member of the Steering Group will regularly check that the filtering methods selected are appropriate, effective and reasonable.
- Staff will maintain visual monitoring whenever a child is accessing the Internet during lessons and ensure they are positioned where they can view the computer or iPad screens.
- Staff will have training and be provided with regular updates to ensure they are kept up to date with what they should be monitoring.
- Computers are set to log off automatically after 30 minutes of non-use.
- Visitors to the school will be requested to read a summary of the schools online safety policy and guidelines when they sign in.

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.
- A group policy is set so only the Admin User can install new software.

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 network users must read and sign the 'Portable Computing Device and Removable Media Security Policy' and 'Computing code of Conduct' Agreement before using any school computing resource.
- The school will maintain a current record of all users who are granted access to school computing systems.
- The school will teach online skills to the children and any breach will be dealt with by following the school's behaviour policy. We have taken the decision that Parents will not be asked to sign an 'Acceptable Use Agreement' as the children are learning how to use computing and therefore fits into our current behaviour policy.
- Access to the Internet for children will be by adult demonstration. This will be followed with directly supervised access to specific, approved on-line materials and any searches undertaken by them will be made using the default search engine KidRex, a child-friendly search engine. Adult login accounts have access to Google and adults will demonstrate how to use this safely during lessons. Computers during this time will not be left unsupervised.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked 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.
- The school will audit computing using to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a member of the steering group.
- Any complaint about staff misuse must be referred to the headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Children and parents will be informed of the complaints procedure and any misuse that has occurred.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school Online Safety Policy.
- Visitors to the school will be given a restricted login and password with restricted access to the school system.
- Only agreed parties have access codes given for the schools Wi-Fi to use on personal devices. These codes expire after a set number of hours.

Communicating the Policy

Introducing the Online Safety Policy to children

- Appropriate elements of the Online Safety Policy will be shared with children.
- Online safety rules will be posted next to the computers.
- Children will be informed that teachers monitor their use when accessing the school network on Internet.
- Curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for children.

Staff and the Online Safety Policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school web site.
- Parents can access the CEOP website (Child Exploitation and Online Protection Command) can be accessed from the school website Home page, to report any online safety concerns.
- Parents and carers will regularly be provided with additional information on online safety.