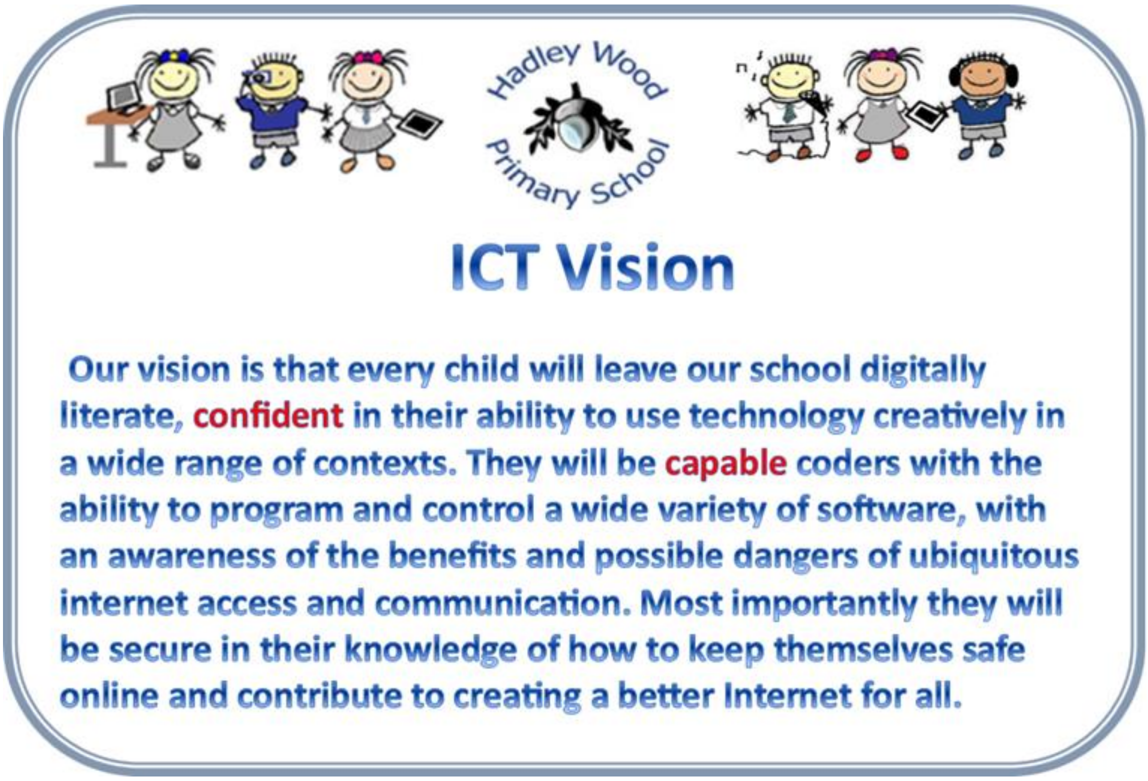
e Safety Policy


Hadley Wood Primary School

ICT Vision

Our vision is that every child will leave our school digitally literate, confident in their ability to use technology creatively in a wide range of contexts. They will be capable coders with the ability to program and control a wide variety of software, with an awareness of the benefits and possible dangers of ubiquitous internet access and communication. Most importantly they will be secure in their knowledge of how to keep themselves safe online and contribute to creating a better Internet for all.

Adopted by the Curriculum Sub-Committee

on behalf of the Governing Body

Date: ………………………………………………………………

Signed: ……

The purpose of the E-safety Policy

The purpose of this policy is to ensure that all staff, parents, governors, volunteers and children at Hadley Wood Primary School understand and agree the school's approach to e-safety. The policy relates to other policies including Computing and Technology, Learning and Teaching, Internet Access, Anti-Bullying, Data Protection, Child Protection and Health and Safety.

Our e-Safety Policy has been written by the school. It has been agreed by the Senior Management Team and approved by the Governing Body in May 2018. The e-Safety Policy will be reviewed annually by the Designated Safeguarding Lead in collaboration with the Computing Subject Leader.

E-Safety Policy Overview

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Teaching and Learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children 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 will be designed expressly for pupil use and will include filtering appropriate to the age of the children
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives / rules for Internet use
- Pupils 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 the Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Introducing the e-safety policy to pupils

- E-safety rules will be discussed with the pupils at the start of each year and in line with the units set out in the Computing Scheme of Work
- E-safety posters will be posted close to all computers within the classroom and be prominent in environments such as the Computing Suite, so all users can see them
- Pupils are informed that network and Internet use is monitored and appropriately followed up
- The children receive regular e-safety lessons and are constantly reminded to stay safe online
- Children will be made aware of the ICT Acceptable Use of Technology Agreements (adapted for KS1 and KS2) available as appendices to the Computing and Technology Policy
- The school recognises the additional risks that children with SEN and disabilities (SEND) face online (for example from online bullying, grooming and radicalisation) and will put suitable scaffolding into place to ensure that SEND children are able to stay safe online as outlined in the updated KCSIE documentation

Good Habits

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

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use
- Safe and secure broadband from the London Grid for Learning including the effective management of content filtering
- The school will work with Enfield LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved
- Any material that the school believes is illegal must be reported to appropriate agencies such as LGFL (who are able to block sites) or CEOP (Child Exploitation & Online Protection Centre, who will take action where appropriate

Assessing Risks

- Hadley Wood Primary School will take reasonable precautions to prevent access to inappropriate 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 Enfield Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

- Children are taught to be risk aware not risk averse. Class teachers will ensure children know how to deal effectively with inappropriate material viewed online

Handling e-safety Complaints

- The Headteacher will deal with complaints of Internet misuse as Safeguarding Lead. They may seek advice and guidance from the school Computing Subject Leader and / or Office Manager
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature must be dealt with in accordance with the school Child Protection Policy
- Hadley Wood Primary School's Child Protection Officer will also act as the E-Safety Coordinator as the roles overlap
- Parents wishing to complain about e-safety issues should use the established school complaints procedure
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues

Managing Internet Access

Authorised Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' which covers both school use and social networking protocols

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the school office or the e-safety coordinator or other senior member of staff, who will then contact the LGFL (our internet provider)
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- Pupils should be taught to understand intellectual property rights

Email

- Pupils may not use email in the school
- Pupils and or staff must immediately tell a member of SLT if they receive/gain access to offensive online materials or images online
- All staff must send email communication to parents via the school office. Personal emails to parents are not permitted
- All communication amongst staff using the school email account will be sent within school working hours Monday – Friday to enable a work/life balance is achieved
- Access in school to external personal e-mail accounts may be blocked

- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

School Website

- The contact details on the school website should be the school address, email and telephone number.
- Staff or pupils' personal information will not be published
- The Office Manager, Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include pupils will be selected carefully
- Pupils' names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Parents of new pupils will be made aware of our policy on the usage of digital images of children
- Pupil's work can only be published on the school website where parents have given permission. Work will not be published where the parent/carer has refused permission

Social Networking

- The school will deny access to social networking sites and newsgroups unless a specific use is approved. Children will be strongly advised not to use these at home in line with the Terms of Use linked to each service. Reminders will be shared with parents through the school newsletter and Parent E-Safety Information Sessions delivered by a CEOP accredited trainer
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils will be advised not to place personal photos on any social network space in their termly e-safety lessons
- Pupils will be informed of the importance of not sharing pictures online (of a sexual, naked or semi-naked image or video of themselves) or send sexually explicit messages (sexting) in line with KCSIE recommendations
- Pupils will be informed about 'Cyberbullying' as a form of peer on peer abuse which involves sending inappropriate or hurtful text messages, emails or instant messages and of the appropriate action they would need to take
- Pupils will be educated on the importance of not sending offensive messages, posting malicious material online (e.g. on social networking websites) or sending or posting offensive or degrading images and videos;

- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others

Filtering

The school will work in partnership with the Local Authority, Becta and the Internet Service Provider to ensure filtering systems are as effective as possible

Video Conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call
- Videoconferencing will be appropriately supervised for the pupils' age

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 will not be used for personal use during school time. The sending of abusive or inappropriate text messages is forbidden

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection is installed and automatically updated
- Security strategies will be discussed with the Local Authority

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Any concerns relating to the schools handling of data should be conveyed to the borough appointed Data Protection Officer (DPO).

Communication of Policy

Pupils

- Rules for Internet access will be posted in the media
- Pupils will be informed that Internet use will be monitored

Staff

- All staff will be informed about and given access to the School e-Safety Policy and its importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- On induction all staff will be required to sign an Acceptable Use of Technology Code of Conduct to be kept on their personnel file
- Staff will always use a child friendly safe search engine when accessing the web with pupils

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site

Role of the Governing Body

Every Governor takes a special interest in at least one curriculum area or focus in the school. The governors support the Headteacher and Computing Curriculum Subject Leader and keep up to date with policies, strategies, monitoring and procedures etc. through regular visits. These visits are used to become familiar with e-safety provision and monitor e-safety curriculum delivery and teaching, carry out regular learning walks in collaboration with the Computing Curriculum Subject Leader to promote levels of accountability, challenge and support. Following a governor visit, a written report is submitted to the Computing Curriculum Subject Leader / Headteacher.

Review

The policy will be reviewed at least every year, or as new guidance becomes available to schools from Department of Education (DfE)