New Hartley First School

E-Safety Policy

Status:	**Statutory**
Created/Reviewed	**Summer 2012, 2013, 2014, 2015, 2016**
Next Review:	**Summer 2017**

Rationale

E-safety encompasses the use of new technologies, internet and electronic communication such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

New Hartley's e-safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Security.

Writing and reviewing the e-safety policy

The E-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, bullying and for child protection. Mr. Wright (Head teacher) is the E-Safety Coordinator. This is in line with his responsibility as Designated Child Protection Coordinator. The E-Safety Policy and its implementation will be reviewed annually.

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 students 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 pupils

• Pupils will be taught what Internet use is acceptable and what is not and given clear objectives 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 Internet content

• The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Managing Internet Access

Information system security

• School ICT systems capacity and security will be reviewed regularly.

• Virus protection will be updated regularly.

E-mail

• Pupils may only use approved e-mail accounts on the school system.

• 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

Published content and the School Website

• The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

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

Publishing pupil's images and work

• Photographs 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 Web site or Blog, particularly in association with photographs.

• Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Social networking and personal publishing

• The school will block/filter access to social networking sites unless specific use is approved.

• Newsgroups will be blocked unless a specific use is approved.

• Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Managing filtering

• The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

• If staff or pupils discover an unsuitable site, it must be reported immediately.
Please see the attached flow chart.

• Policy Central Enterprise (PCE) provides a range of tools to monitor and block internet and network usage and provides automatic reports on what activity is taking place on the school network and computers. PCE displays the schools Acceptable Use Policy (AUP) on logon and failure to agree to this means users will not be allowed to use the computers.

Managing videoconferencing

• 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.

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 staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

• The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

• Access to the Internet will be initially by adult demonstration and then with directly supervised access to specific, approved on-line materials.

• Parents will be asked to sign and return a consent 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 will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

• Complaints of Internet misuse will be dealt with by a senior member of staff.

• Any complaint about staff misuse must be referred to the head teacher.

• Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet

• The school will liaise with local organisations to establish a common approach to e-safety.

Communications Policy

Introducing the e-safety policy to pupils

• E-safety rules will be posted in all networked areas and discussed with the pupils at the start of each term.
• Pupils will be informed that network and Internet use will be monitored.

• E-safety training will be provided to all pupils on a termly basis.

Staff and the e-safety policy

• All staff will be given the School e-Safety Policy and its importance explained.

Enlisting parents' support

• Parents' attention will be drawn to the School e-Safety Policy in newsletters, the Home – School Agreement and on the school web site.