Hale Preparatory School E-Safety and Acceptable Use Policy

Teaching and learning

Internet Access

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the Hale Prep curriculum and a necessary tool for staff and pupils.
- Internet use will enhance learning
- The school Internet access will be designed specifically for pupil use and will include filtering.
- Pupils will be taught what Internet use is acceptable and what is not and will be 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.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

E-mail

- When available, pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In any e-mail communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- 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 web site

- Staff or pupil personal contact information will not be published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Pupils' names will not be used in association with photographs anywhere on the school Web site.
- Pictures will only be shown on the website if parents/carers have signed the consent form issued at the start of each school year.
- Parents will be clearly informed of the school policy on image taking and publishing.
- Parents will have access to this policy through the school website, including a link to the Cyberbulling Policy.

Social networking and personal publishing

- In school, social networking sites will not be used.
- During IT e-safety lessons, pupils will be advised to:
    - use nicknames and avatars when using social networking sites at home.
    - Never arrange to meet anyone on a networking site.
    - Not post pictures wearing school uniform.
    - Ask permission of those involved before posting pictures.
    - Only make 'friends' or chat to people they know, and who are of similar age.
    - Never give out ANY information about themselves eg. phone number, address.

Responsibilites

- All staff who uses ICT connected with the school has a responsibility to have a regard for e-safety. It is NOT just the remit of the Headteacher/IT teacher.
- The teaching staff have a responsibility to teach e-safety.
  The e-safety / IT teacher(s) will:
- oversee the review of this policy
- oversee the implantation of this policy
- advise the school management on e-safety issues
- advise staff on e-safety teaching and learning resources
- be a point of contact for any concerns about e-safety.
- Pass onto the Headteacher any complaints received concerning individuals or staff misuse of ICT
- Supervise the technician who manages the filtering systems/security systems.
- Teach a block of 'e-safety' lessons, in addition to ongoing instruction.
- Ensure that all staff read and sign the "Acceptable Use of ICT - Staff" document before using any school ICT resource. This is to be renewed at the start of each new school year (normally in September).

Technical provision

- Hale Prep has “ESET End Point Security” installed on all of its computers to combat any possible virus’. It also has Censornet SWG to filter and monitor inappropriate content, to fulfil all of the school’s safeguarding obligations. This is updated every evening. This will keep children safe from terrorist and extremist material when accessing the internet through school systems.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Every member of staff must take all reasonable steps to securely protect all data concerning pupils and others.
- Any data taken off the school premises should be kept to a minimum and if no longer required, deleted or destroyed in an appropriate manner, or returned to school for destruction.
- All printed copies of personal data must be shredded before disposal as waste material.
- Staff must take all reasonable care when using, storing and transporting memory sticks, CDs or DVDs containing school data.

Reviewed February 2017