E-Safety Policy

HAZELMERE Junior School

1 Writing and Reviewing the e-Safety Policy

Our e-safety policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors. Our school has appointed an e-Safety Co-ordinator (Jayne Bond). The school has appointed a member of the Governing Body to take lead responsibility for e-Safety.

The e-safety policy and its implementation will be reviewed annually.

2 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 pupils with quality internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary tool for learning.

- Pupils use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security.

- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

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 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.

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

3 Managing Internet Access

Information system security

- Schools ICT systems security will be reviewed regularly.

- Virus protection will be updated regularly.

- Portable media may not be used without specific permission followed by an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email
- Files held on the school network will be regularly checked
- The ICT co-ordinator/technician will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

E-mail

- Pupils may only use e-mail accounts provided through our VLE – Learn Anywhere and on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail, although Learn Anywhere filters protect the children to a large degree.
- Pupils must not reveal any personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation 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.

Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The school website will comply with the school's guidelines for publication including respect for intellectual property rights, privacy policies and copyright.

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 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.
- Pupils' work can only be published with the permission of the pupil and parents.
- The school will have a policy regarding the use of photographic images of children which outlines policies and procedures.

Social networking and personal publishing

- The school will block/filter access to external social networking sites and will allow the children 'School Jotter' through the Learn Anywhere site. This will develop skills in keeping themselves safe whilst social networking in a controlled setting.

- 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.

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.

- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

- Concerns regarding students' use of social networking, social media, and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

Managing filtering

- The school will work with the LA 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 to the e-safety co-ordinator.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.

- Staff will use a school phone where contact with pupils/parents is required.

- All video conferencing equipment in the classroom must be switched off when not in use.

- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use of Mobile Phone Policy.

Protecting personal data

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

4 Policy Decisions

Authorising Internet access

- All staff must read and sign the HR Schools Service – Code of Conduct Policy issued by Essex County Council.

- 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.

- 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. Neither the school nor the LA can accept liability for the material accessed, or any consequences on internet access.

- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling e-safety complaints

- Complaints of internal internet misuse will be dealt with by a senior member of staff.

- 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.

- Pupils and parents will be informed of the complaints procedure.

- Discussions will be held with the community policy to establish procedures for handling potentially illegal issues.

Community use of the internet

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Managing Cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying as a result of using the VLE and internal sites.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of internal cyberbullying.
- Pupils/staff/parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting Learn Anywhere (provider of the VLE) and police, if necessary.
- Pupils, staff, and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-safety ethos.

Managing Learning Platforms

- Only members of the current pupil, parent/carers and staff community will have access to the Learning Platform (VLE).

- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

5 Communications Policy

Introducting the e-safety policy to pupils

- E-safety rules will be posted in the ICT suite and discussed with the pupils at the start of each year.

- Pupils will be informed that network and internet use will be monitored.

Staff and the e-safety policy

- All staff will be given 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.

- To protect all staff and pupils, the school will implement Acceptable Use policies.

- Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff.

- All staff members will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-safety at home and at school with parents will be encouraged. This may include offering parent sessions with demonstrations and suggestions for safe home internet use.
- Parents will be requested to sign an e-safety/internet agreement as part of the Home School Agreement.
- Information and guidance for parents on e-safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the internet will be made available to parents.
- Interested parents will be referred to organisations listed in the 'e-safety' section of the school website.

Failure to comply

- Failure to comply in any way with this policy will be considered a serious risk to health and safety and all incidents of non-compliance will be investigated by a senior member of staff.

Signed:

Date:

Review: