Henley Green Primary School

E-safety Policy
September 2016

1. The Policy

This Internet Policy has been written by the School’s IT Manager and Deputy Head Teacher in February 2010 and revised by the IT Manager in January 2014 and September 2016. Governors have approved the policy. Changes will be made immediately if technological or other developments so require. The policy is amongst the safe guarding measures that the school takes to ensure the provision of safe and effective care of our school community. The intention of the school is to strengthen its strategies for safeguarding pupils and the promotion of e-safety to children and young people. Internet Safety and the protection of children is the responsibility of the whole school and e-safety should not be the sole responsibility of the IT Manager or technician. Reference to e-safety is also made in other policy documents such as the Teaching and Learning Policy, Behaviour Policy and the English Policy. This is to ensure e-safety is an integral part of all areas of learning.

2. Why is Internet use important?

- 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 information and business administration systems.
- Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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.

3. How does the Internet benefit education?

Benefits of using the Internet include:
- Access to world-wide educational resources including museums and art galleries
- Inclusion in Government initiatives
- Inclusion in Local initiatives
- Educational and cultural exchanges between pupils world wide
- Access to experts in many fields for pupils and staff
- Development of a more effective form of interschool communication tool
- Staff professional development through access to national developments, educational materials and planning tools
- Communication with support services, professional associations and colleagues; improved access to technical support including the remote management of networks
- Exchange of curriculum and administration data between school, Local Authority or DCSF.
4. How will Internet use 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 is acceptable and what is not acceptable and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend the learning outcomes planned for the pupils’ age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills knowledge location and retrieval.

5. How will pupils learn to evaluate Internet content?

- If staff or pupils discover unsuitable sites the URL (address) and content must be reported to the Internet Service Provider via the IT Manager, Deputy Head or Head Teacher. Pupils should inform the first available teacher if they find unsuitable sites. The instance will be recorded in the Internet Incident Log on the Staff Resources Site.
- The school should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught how to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to acknowledge the source of information and to respect copyright when using Internet material in their own work.

6. How will e mail be managed?

- Pupils may only use approved e mailing accounts such as e pal. Anonymous systems such as Hotmail will not be allowed.
- Pupils are aware of their responsibility to using e mail responsibly and sign an e usage agreement referring to responsibilities and consequences.
- Pupils are not to give out their e mail user account details to outside agencies/persons, unless authorised by a teacher.
- User accounts can and may be tracked by the IT Manager/Head Teacher.
- Pupils must immediately tell a teacher/adult if they receive offensive e mail. The instance will be recorded in the Internet Incident Log on the Staff Resources Site.
- Pupils must not reveal details of themselves or others, such as address, telephone number, or arrange to meet anyone in e mail or any other electronic communication.
- Excessive social e mail can interfere with learning and is restricted.
- E mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter sent on school headed paper.
- The forwarding of chain letters is not allowed.

7. How should the School’s Website content be managed?

- The point of contact on the Website should be the school address, school e mail and telephone number. Staff or pupils’ home information will not be published.
- Website photographs that include pupils will be selected carefully and will not be used without parental consent.
- Pupils’ names will not be used on the Website when associated with photographs.
- Pupils photographs will immediately be removed from the school website upon parent request.
- Pupils’ work will only be published with first name attached.
- The IT Manager will take overall responsibility and ensure content is appropriate and accurate. The Website should comply with the school’s guidelines for publications.
- The copyright of all material must be held by the school, or attributed to the owner where permission to reproduce has been obtained.
8. How can emerging Internet uses be managed?

- The school’s website is regulated by the E-safety Policy, User Agreements, E-Safety training for staff, pupils and parents.
- These sessions and policies will be developed and co-ordinated by the IT Manager and Deputy Head Teacher.
- Emerging Technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The sending of abusive or offensive electronic communications is not allowed.

9. How will Internet access be authorised?

- All staff and pupils will have Internet access in school
- Parents will be informed that pupils will be provided with supervised Internet access
- Parents will be informed that the school’s website is a learning tool for home and Parent Information sessions will be held to inform parents of its virtual safety and other aspects of Safety on line.
- Pupils will not be allowed to use computers with Internet access unsupervised.

10. How will the risks be assessed?

- In common with other media, such as magazines, books and dvd, some material available via the Internet may be unsuitable for children. 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 cannot accept liability for the material accessed, or any consequence of Internet access.
- The school has in place the recommended filter service Red Stone and forensic software (Policy Central Enterprise-PCE) to help regulate the safety of the Internet for all of the school community.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly by the Head Teacher and IT manager.
- The Head Teacher will ensure that the Internet Policy is implemented and compliance with the policy monitored.

11. How will filtering be managed?

- The school will work in partnership with parents, the Local Authority, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites the URL (address) and content must be reported to the Internet Service Provider via the IT Manager, Deputy Head or Head Teacher. Pupils should inform the first available teacher if they find unsuitable sites. The instance will be recorded in the Internet Incident Log on the Staff Resources Site.
- Leadership will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The forensic software (PCE) is a highly effective and interactive management tool, playing a key role in helping to deliver and maintain a school wide ethos of e safe behaviour. It will report any incidents that contain inappropriate content.
12. How will the policy be introduced to pupils?

- Rules for Internet access will be posted on or near all computer systems with Internet access.
- Internet Safety guidelines will be prominently linked on the website.
- Pupils will be informed that Internet use will be monitored.
- E safety will be taught through the appropriate curriculum for all pupils and will precede Internet access, through the school’s e safety programme.
- A “Safe Thinking” learning power will be linked to Henley the dog as one of our Elli animals. This will support children in understand how to be safe in a variety of situations.
- Children will have their own log-ins and passwords to support them in learning that they must respect others’ privacy. This will also enable the Head Teacher and IT Manager to monitor Internet use.

13. How will staff be consulted?

- All staff must accept the terms of the ‘Responsible use of the Internet’ statement before using any Internet resource in school. The Head Teacher will retain the signed copy.
- All staff will be provided with the School E-Safety Policy and its importance explained through staff training.
- Staff should be made aware that Internet use can be monitored through the Forensic Software and traced to individual users. Discretion and professional conduct is expected.
- The monitoring of Internet use is a sensitive matter and will only be conducted by the Head Teacher with the IT Manager.
- Staff development in safe and responsible Internet use and on school Internet Policy will be provided as required.

14. How will the school’s IT system’s security be maintained?

- The school’s IT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security Strategies will be discussed with the LA, particularly where a wide area network connection is being planned.
- Unapproved system utilities and executable files will not be allowed in pupils’ work areas or attached to e mail.
- Files held on the school’s network will be regularly checked.
- The IT Manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

15. How will complaints regarding Internet use be handled?

- Responsibility for handling incidents is delegated to the IT Manager.
- Any complaints about staff misuse is referred to the Head Teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will work in partnership with the school to resolve issues.
- Police may need to be contacted to establish the legal position and discuss strategies.
- Sanctions available include:
  - Interview with head teacher
  - Informing parents or carers
  - Removal of internet/computer access
16. How will parents’ support be enlisted?

- Parents’ attention will be drawn to the School Internet Safety Policy via: Henley Green Website, Parent Support Leaflet, Parent Information Session and the school Newsletter.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home.
- www.henleygreen.co.uk will prominently promote safe Internet use.

Last Reviewed September 2016