HIGHBURY PRIMARY SCHOOL

GOVERNORS' E-SAFETY POLICY

Highbury Primary and Nursery School's mission is:

- To be an inclusive, safe and caring community where each member is equally valued and nurtured to develop their potential.
- To achieve academic excellence by ensuring each pupil performs to the best of their ability.
- To work together as a team with parents and carers within the community to promote respect responsibility for the benefit of all.

E-Safety Policy

Writing and reviewing the e-safety policy

The E-Safety Policy forms part of a range of policies for safeguarding and ICT.

- The school will appoint an E-Safety coordinator. The E-Safety coordinator works closely with the Designated Child Protection Coordinator as the roles overlap.
- Our E-Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The E-Safety Policy and its implementation will be reviewed bi-annually.
- The E-Safety Policy was revised by Wendy Fowler
- It was approved by the Governors on: November 2017
- To be reviewed: November 2019

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 is provided by Drift and includes filtering appropriate to the age of pupils. An additional filtering set is available in school administration networks only and enables staff access to additional resources.
- 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

- Schools should ensure that the use of Internet derived materials by staff and by 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.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Chichester Academy Trust.

E-mail

- Pupils and staff 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.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- 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 web site

- 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 Headteacher or nominee 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 unless parents give written permission for this.
- Pupils' full names will not be used anywhere on the Web site or learning platform including in blogs, forums or wikis, 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 on the school learning platform

- Drift will normally block/filter access to social networking sites unless short-term access is required for a specific educational project.
- 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 is inappropriate for primary aged pupils.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Managing filtering

- The school will work in partnership with Drift to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to Drift Help Desk immediately.

Managing videoconferencing

- 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 during lessons or formal school time. The sending of abusive or inappropriate messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

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 'Staff Information Systems Code of Conduct' before using any school ICT resource.
- The school will work with Highbury College to maintain a current record of all staff and pupils who are granted access to school ICT systems.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Drift can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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's safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school e-safety policy.

Communications Policy

Introducing the E-Safety policy to pupils

- E-Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- The school will ensure that online safety is included in relevant lessons and that children are taught about safeguarding, including online, through teaching and learning opportunities.

Staff and the e-Safety policy

- All staff will be directed 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.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers attention will be drawn to the school e-Safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on e-safety.

Approved by the Governing Body: ……

Date implemented: November 2017 Review Date: November 2019