ABU HANIFAH FOUNDATION

Excellence in Islamic Education

"Where every child matters"

E-Safety Policy

Updated September 2019-20

Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Data Protection and Safeguarding.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- The signing of the 'Acceptable Internet Use' policy by all staff members.
- Use of the school's ICT software.
- Education of pupils through E-Safety timetabled on the curriculum

The school has appointed an e-Safety coordinator this will be the Designated Child Protection Officer as the roles overlap.

Why is Internet Use Important?

The purpose of Internet use at Abu Hanifah Foundation 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 administration systems.

Internet use is part of the curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality and appropriate internet access.

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

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and teaching resources;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- All AHF staff are trained on how to monitor student's internet access
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support 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 of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Deputy Principal or Principal.
- AHF will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- The staff school email system is hosted by googlemail.
- AHF does not currently provide 'in-house' email facilities for our pupils.
- Pupils are not allowed to check any personal email accounts within the ICT suite and these sites can indeed be blocked by staff, thereby ensuring our PC's are not harmed by any external viruses.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received, professional conduct when sending emails using a school e-mail address is expected at all times.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media at all times;
- Posting anonymous messages and forwarding chain letters is forbidden;

Social Networking

- At AHF access to social networking sites and newsgroups are currently available but controlled by the teacher's use.
- Pupils, though advised not to use social networking sites, either at school or indeed at home, are however advised never to give out personal details of any kind which may identify them or their location.

- Pupils are advised not to place personal photos on any social network space.

Internet Filtering

The school filters undesired material through a DNS Filter Network System. The on-going success is reviewed termly by the safety coordinator.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use at AHF is allowed.
- Pupils are not allowed to bring or therefore use mobile phones for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff are not allowed to use their mobile phones either in class, or whilst walking around the school.

Published Content and the School Web Site

AHF maintains to follow our existing e-safety standards:

- 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 Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' 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 Social Media, 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.

Information System Security and Virus Protection

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly. The PC's in the ICT suite have been recently reviewed and reinstalled with 'Anti-Virus and Malware Protection'.
- Staff laptops and PC's in the main building of the school are protected by 'Microsoft Security Essentials', set to run a virus scan once weekly. This scan is regularly reviewed by the ICT coordinator.
- Newer computers have Norton Anti-Virus installed on them.

Protecting Personal Data

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

Assessing Risks - on-going

- 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. No internet content filtering system is 100% secure due to the ever changing nature of undesirable sites, virus or material.
- The school should 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 or deputy head teacher.
- 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.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

- 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.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

AHF E-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

AHF INFORMATION SYSTEMS CODE of CONDUCT

To ensure that the staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct, in conjunction with our 'Acceptable Internet Use' policy. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the head teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …….. Date: ……