ASHLEY HIGH SCHOOL

E-SAFETY POLICY

Written by A.Ivins, December 2009

Updated January 2018.

E-Safety Policy

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.

Good Habits

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

- Responsible ICT use by all staff and students; 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.
- Safe and secure broadband from Halton Borough Council, including the effective management of content filtering.

School E-Safety Policy

The E-Safety Policy has been written by the ICT Coordinator – Mrs A. Ivins. It has been agreed by the staff, the senior management team and the school governors.

The E-Safety Policy will be reviewed annually. This policy will next be reviewed in January 2019.

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote student 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 statutory 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 students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality Internet access.

Students 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 learning wherever and whenever convenient.
- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students 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.
- Exchange of curriculum and administration data with the Local Authority and DCSF.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for student use and includes filtering appropriate to the age of students.
- Students 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 students in on-line activities that will support learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

E-Safety Education
Students

To equip students as confident and safe users of ICT the school will undertake to provide:

- A planned, broad and progressive e-safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years.
- Regularly auditing, review and revision of the ICT curriculum
- E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner
- Opportunities for students to be involved in e-safety education e.g. through peer mentoring

Additionally,

- Students are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information

- There are many opportunities for students to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- The school actively provides systematic opportunities for students to develop the skills of safe and discriminating on-line behavior
- Students are taught to acknowledge copyright and intellectual property rights in all their work.

Staff

- A programme of formal e-safety training is made available to all staff if needed. Additionally, all staff have had CPD on the Prevent duty.
- E-Safety training is an integral part of Child Protection / Safeguarding training and vice-versa
- All staff have an up to date awareness of e-safety matters, the current school e-safety policy and practices and child protection / safeguarding procedures
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy which tjey then sign
- The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety
- The school takes every opportunity to research and understand good practice that is taking place in other schools
- Governors are offered the opportunity to undertake training.

Authorised Internet Access

- The school will maintain a current record of all staff and students 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 students will be provided with supervised Internet access.
- Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.
- Students must always be supervised by a member of staff when using the Internet or any other online resource in school.

World Wide Web

- If staff or students discover unsuitable sites, the URL (address), time and content must be reported to the Local Authority helpdesk via the ICT Coordinator and Office Manager.
- Ashley High School will ensure that the use of Internet derived materials by students and staff complies with copyright law.
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

- Students are encouraged to use safe online educational resources at home.

Email

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or to arrange to meet anyone without specific permission.
- Students do not have permission to access external e-mail accounts in school.
- E-mail sent to external organisations 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.

Data Storage

We do not allow students to bring in USB pens from home and use them on school computers. Students must only use USB pens provided by the school.

Social Networking

- Students do not have permission to access social networking sites such as Facebook and Youtube.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students should be advised not to place personal photos on any social network space.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Access to chat rooms is not permitted in school.

Mobile phones and other devices

School recognizes that staff may need to have access to mobile phones on site during the working day. School allows staff to bring in mobile phones for their own personal use. However, they must be kept securely at all times and are not allowed to be used in the toilets, changing rooms or in the play areas at any time. If staff fail to follow this guidance, disciplinary action will be taken in accordance to the school's staff code of conduct. If staff need to make an emergency call, they must do so either in the main or Headteacher's office. Staff must ensure that there is no inappropriate or illegal content on the device.

Mobile phone technology may not be used to take photographs anywhere within the school grounds. There are digital cameras and iPads available within the school and only these should be used to record visual information within the consent criteria guidelines of the local authority and the school.

Members of staff may only contact a parent / carer on school approved mobile phones.

Students should not use mobile phones within the school grounds.

Use of Mobile Phones for Volunteers and Visitors

Upon their initial visit volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises. If they wish to make or take an emergency call they may use either the main or the Headteacher's office. Neither are volunteers or visitors permitted to take photographs or recordings of the children without the Headteacher's permission. In order to safeguard children and adults and to maintain privacy, cameras are not to be taken into the toilets by adults or children. All adults whether teachers / practitioners or volunteers at the school understand the difference between appropriate and inappropriate sharing of images.

All images are kept securely in compliance with the Data Protection Act.

If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated but staff should not 'search' the phone. The incident should be passed directly to LMT who will deal with the matter in line with normal school procedures.

Filtering

The school will work in partnership with the Local Authority and Websense to ensure filtering systems are as effective as possible.

The Prevent Duty

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

The Prevent Duty requires a schools monitoring and filtering systems to be fit for purpose.

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 for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- A school mobile phone is used for off-site staff on trips to communicate with school during school hours.

Publishing Students' Images and Work

- Photographs that include students will be selected carefully and will be appropriate for the context.
- Students' full names will not be used in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the Website.

- Staff should always use a school camera to capture images and should not use their personal devices.
- Photos taken by the school are subject to the Data Protection Act.
- Work can only be published with the permission of the student.

Photos and videos taken by parents/carers.

- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos / videos from school events on social networking sites if other students appear in the background.
- Parents attending school based events will be reminded of their responsibilities in relation to social media verbally and through notices.

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 Local Authority.

Protecting Personal Data

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

I will ensure that all data regarding students and staff, financial information and any information classified as confidential (including all data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Student / teacher / any school confidential data can only be taken out of school or accessed remotely away from school when authorised by the Head.
I will not save any documents to a non-school PC or print to a non-school printer.

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 Halton Borough Council 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.

Reporting

All breaches of the E-Safety policy need to be recorded in the ICT Reporting Book that is kept in the ICT room. The details of the user, date and incident should be reported. Incidents which may lead to child protection issues need to be passed on to the designated teacher immediately.

Incidents that are of a concern under the Prevent duty should be referred to the designated lead immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary, the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum covers how students should report incidents.

The teachers, as part of their normal class discipline, may deal with minor transgressions of the rules. However, in more serious cases:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Students and parents will be informed of the complaints procedure.

The impact of the e-safety policy and practice is monitored through the review of:

- ICT reporting book (e-safety incident records)
- incident/behaviour logs
- Safeguarding audit by Halton Safeguarding Children Board

The records are reviewed and reported to:

- School's senior leaders including the Safeguarding Team
- Governors (as part of Safeguarding termly report)
- Halton Local Authority (where necessary)

Communication of Policy

Students

- Rules for Internet access will be available around the school, including classrooms and the ICT suite.
- Students will be informed that Internet use will be monitored.

Staff

- All staff will be made aware of 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.

Parents

- Parents' attention will be drawn to the School e-safety Policy in newsletters, at parents' meetings and on the Website.

E-Safety Rules

These E-Safety Rules help to protect students 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. All inappropriate web pages should be closed and reported to a teacher immediately.
- Internet chat rooms / MSN should not be used in school.
- Copyright and intellectual property rights must be respected.
- Messages and e-mails 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, and should never arrange to meet anyone we don't know.
- The school ICT systems may not be used for private purposes, unless the Headteacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

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