King Edward VI Aston School

E-Safety Policy

This policy applies to all members of the school community who have access to and are users of school ICT systems – staff, students, volunteers, parents, visitors.

1. AIMS

i. To ensure that students, staff, volunteers and parents are able to use the internet and related communication technologies appropriately and safely.
ii. To build students' resilience to risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.
iii. To provide the necessary safeguards to manage and reduce risks.
iv. To help students, staff, volunteers and parents to be responsible users and stay safe using the internet and other communication technologies for educational, personal and recreational use.
v. To safeguard students and staff.

2. CONTEXT

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. They help teachers and students to learn from each other. Young people should have an entitlement to safe internet access at all times. Though the use of these innovative technologies can help to raise educational standards, nevertheless they can also put young people at risk. Some of the dangers they may face include:

i. Access to illegal, harmful or inappropriate images
ii. Unauthorised access to, loss of, or sharing of personal information
iii. The risk of being groomed by those with whom they make contact on the internet
iv. Sharing or distribution of personal images without an individual's consent or knowledge
v. Inappropriate communication or contact with others, including strangers
vi. Cyber-bullying
vii. Access to unsuitable video or internet games
viii. An inability to evaluate the quality, accuracy and relevance of information on the internet
ix. Plagiarism and copyright infringement
x. Illegal downloading of music or video files
xi. The potential for excessive use which may impact on the social and emotional development and learning of students.

3. REPORTING MISUSE

It is impossible to eliminate risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the skills and confidence to deal with these risks. It is also essential for the school to have effective procedures to report misuse and it is the school's responsibility to ensure the students are aware how to report any incidents of misuse or concern through use of the school's reporting system:

The system is called S.H.A.R.P (School Help Advice Reporting Page).

The S.H.A.R.P system has been designed as a number of web pages which can be used as an education tool as well as providing the means to report incidents securely and confidentially. Incidents can be reported by students, staff, parents or members of the local community. It is accessed through the links on both the school website and the VLE. Any modern Internet enabled device can be used to access this reporting system.

The system is promoted via the following means:

i. Whole school and year group assemblies
ii. Staff INSET
iii. Emails to students via school internal email system
iv. Advertised on Plasma TV Screens around the school
v. Letters to Parents
vi. Demonstrations of the system for students in ICT lessons
vii. SHARP system link on school web home page & VLE
viii. SHARP system icon on staff desktop in school
ix. Use of the SHARP system during parents' evenings and open days
x. Use of School Bulletins to raise awareness
xi. Posters around the school highlighting the system

4. ROLES AND RESPONSIBILITIES

a) Governors

i. Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy annually.
ii. Governors will appoint an e-safety governor. This role involves regular meetings with the e-safety officer (currently the DSL) and reporting to the full Governing Body.

b) Head Master

i. Ensuring the safety of members of the school community, though the day to day responsibility will be delegated to the e-safety officer (DSL).
ii. Ensure the e-safety officer (DSL) has access to up to date professional development.

iii. Make sure there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
iv. Receive regular monitoring reports from the e-safety officer (DSL).
v. Implement the policy in the event of a serious e-safety allegation being made against a member of staff.
vi. Deal with any staff disciplinary issues which may arise / be reported.
vii. Receive and review reports from the ICT/e-safety committee and ensure that e-safety updates are included as an agenda item at each committee meeting.

c) E-Safety Co-ordinator / DSL – Safeguarding:

i. Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy.
ii. Liaises with school ICT technical staff.
iii. Acts as the key contact for the S.H.A.R.P reporting system.
iv. Ensures that all staff are aware of the procedures that need to be followed in order to promote effective e-safety within school.
v. Ensures that staff are trained and advised on e-safety issues.
vi. Reviews a log of incidents provided by the Network Manager and reports to the Headmaster.
vii. Meets regularly with the e-safety governor.
viii. As DSL be aware of the potential for serious child protection issues to arise from:
    - Sharing personal data
    - Access to illegal/inappropriate materials
    - Inappropriate on-line contact with adults/strangers
    - Potential or actual incidents of grooming
    - Cyber-bullying

d) Network Manager

i. Make sure the ICT infrastructure is secure and not open to misuse or malicious attack.
ii. Make sure users can only access the school's networks through a properly enforced password protected system.
iii. Keeps up to date with e-safety technical information.
iv. Regularly monitors the network in order that any misuse or attempted misuse **by students** is reported to the E-Safety Co-ordinator (DSL), and **by staff** is reported to the Headmaster.
v. Produces and maintains a log of incidents for the E-Safety Co-ordinator (DSL).

e) Teaching and Support Staff

i. Have up to date awareness of e-safety matters and understand the e-safety policy.
ii. Have read, understand and signed the Staff Acceptable Use Agreement.
iii. Report any suspected misuse or problem to the e-safety officer (DSL).
iv. Have an awareness of, and promote the use of the SHARP reporting system.

v. Digital communication with students should always be on a professional level and only carried out using school systems.
vi. Ensure students understand and follow the school e-safety and acceptable use policy.
vii. Ensure students understand research skills and the need to avoid plagiarism and uphold copyright regulations.
viii. Monitor ICT activity in lessons.
ix. Be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices.
x. In lessons, guide students to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

f) Parents/Carers

i. Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.
ii. The school will help parents to understand e-safety issues through, parental training sessions, the school website and promotion of the SHARP reporting system.
iii. Parents should be aware of the school policy on e-safety and the school Acceptable Use agreements.
iv. By accepting the parental username and password to the school's Moodle system they agree to comply with the terms of the school's Acceptable Use Agreement.
v. Parents should be aware of how to report concerns or misuse through the SHARP system.

g) Students

i. Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Agreement which must be read and agreed to before accessing the school network.
ii. Have a good understanding of personal research skills and the need to avoid plagiarism and uphold copyright regulations.
iii. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so through the SHARP reporting system.
iv. Are expected to know and understand school policies on the use of mobile technologies.

5. Education and Training

a) Educating students about e-safety

The school will ensure that:

i. An e-safety programme is provided as part of the ICT programme

ii. The PSHEE curriculum will have a number of dedicated e-safety lessons each year for every year group of students
iii. Assemblies will frequently re-visit the issue of e-safety
iv. Students, where appropriate, are taught to be critically aware of the materials they access and be guided to validate the accuracy of information
v. Students are encouraged to adopt safe and responsible use of ICT and to respect copyright when using materials accessed on the internet or through the VLE
vi. Students are aware of how to use the SHARP reporting system and how to access it through the website and VLE.

b) Educating parents about e-safety

The school will help parents to understand e-safety issues through parental training sessions, the school website and promotion of the SHARP reporting system.

c) Staff training

i. All new staff should receive e-safety training as part of their induction programme, ensuring they understand the school e-safety policy and sign the Acceptable Use Agreement.
ii. All staff will have the opportunity to identify e-safety as a training need within the performance management process.
iii. The e-safety co-ordinator (DSL) will receive regular updates through attendance at external training sessions and by reviewing guidance documents issued by the DfE and other organisations.

6. Technical infrastructure

i. The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible.
ii. E-Safety updates will be a standing agenda item at each meeting of the ICT/e-Safety Committee.
iii. Servers, wireless systems and cabling must be securely located and physical access restricted
iv. All users will have clearly defined access rights. Details of the access rights will be recorded by the Network Manager.
v. All users will be issued with a username and password for systems and services to which they are allowed access by the IT Department. Users are responsible for the security of their username and password.
vi. The school maintains and supports a managed filtering service which filters content entering the school's network.
vii. School ICT technical staff regularly monitor and record the activity of users on the school ICT systems.
viii. Appropriate security measures are in place to protect servers, firewalls, routers, wireless systems, work stations and hand held devices from accidental or malicious access attempts which might threaten the security of the school systems and data.

ix. Temporary access for guests is available. This has very limited access to Internet Services only.
x. The school infrastructure and individual workstations are protected by up to date antivirus software.
xi. The school uses a filtering system which blocks sites that fall into categories such as pornography, homophobic, race hatred, gaming, social networking, extremism etc.

7. Use of digital and video images

i. Staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet.
ii. When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites (see separate guidance for staff on the use of social networking).
iii. The personal equipment of staff should not be used for taking digital images.
iv. Care should be taken when taking digital/video images that students are appropriately dressed.
v. Students and staff must not take, use, share, publish or distribute images of others without their permission, or in the case of a student without parental permission.
vi. Students' full names will not be used anywhere on the website, particularly in association with photographs without first having the permission of parents and the Headmaster.
vii. Written permission from parents will be obtained each year regarding the use of photographs of students in internal and external displays, publicity and promotional material (e.g. web site and press releases) by the school and occasionally by the Schools of King Edward VI Birmingham Foundation.
viii. The school makes every attempt to block access to social networking sites.
ix. We have CCTV in school as part of our site surveillance for student and staff safety. It may be necessary for senior staff to view recordings as part of school based investigations. We will not provide copies of any recordings except where disclosed to the police as part of a criminal investigation.

8. E-mail

i. The school email service may be regarded as safe and secure and is monitored by way of screening messages.
ii. Users must immediately report to their teacher or the e-safety officer (DSL) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature, and must not respond to such material. The SHARP system can be used to report these concerns.
iii. Any digital communication between staff and students, pupils or parents, must be professional in tone and content and will be monitored.

iv. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
v. Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
vi. SIMS InTouch should be used to send emails, or 'bcc' used for all recipient email addresses.

9. Protecting Personal Data

Personal Data will be recorded, processed, transferred and made available according to the Data Protection Act, 1998 (see the school's Data Protection Policy) and new GDPR regulations.

10. Responding to incidents of misuse

i. In most cases, the E-safety Officer (DSL) should be the first point of contact for any complaint.
ii. Complaints and or incidents of misuse should be reported through the SHARP system.
iii. Any complaint about staff should be reported to the Headmaster.
iv. Complaints about cyber-bullying are dealt with in accordance with the school Anti-Bullying Policy.
v. Complaints related to Safeguarding and Child Protection are dealt with in accordance with the school Safeguarding Policy.
vi. Incidents of mobile phone misuse will be dealt with in accordance with the school policy concerning the use of mobile phones.

11. Monitoring and review process

i. The e-safety policy will be reviewed annually.
ii. The E-safety co-ordinator (DSL) will monitor the implementation of the policy
iii. The Headmaster will report to governors about e-safety incidents and will discuss any significant new developments with the e-safety governor.

Linked Policies:
Anti-bullying Policy
Safeguarding Policy
Data Protection Policy
Student Behaviour Policy
Staff Behaviour Policy
Policy for the use of mobile phones and other portable electronic devices
Related Documents:
Student Acceptable Use Agreement (see appendix 1)
Staff (and Volunteer) Acceptable Use Agreement (see Appendix 2)
Letter to parents and carers including VLE username and password
Acceptable user agreement for parents and carers (see Appendix 3)

Policy approved: 23rd January 2017

APPENDIX 1

Student/Staff/Volunteer Acceptable Use Agreement

• In order to safeguard students and staff it is important that all computer system users take all possible measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All staff and students have a responsibility to use the school's computer system in a professional, lawful and ethical manner.
• School owned information systems must be used appropriately. I understand that the Computer Misuse Act, 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
• I understand that any hardware and software provided by the school for staff and student use can only be used by members of the school and only for educational use/practice. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking the computer as appropriate.
• I will respect system security and I will not disclose any password or security information. I will not give anyone access to a computer system which I have gained access to. I will use a 'strong' password (including letters and numbers).
• I will not attempt to install any purchased or freely downloaded software, including browser toolbars, or hardware without permission from the IT systems manager.
• I am aware of the school's General Data Protection Regulation (EU) 2016/679 (GDPR) Privacy Notice and Data Protection Policy available from the King Edward VI Academy Trust and Aston school website - https://www.schoolsofkingedwardvi.co.uk/legal-information/
• I have read and understood the school e-safety policy.
• I will report all incidents of concern to the school e-safety co-ordinator / DSP.
• If I access school emails on a personal device, I will ensure that the device is 'at least' password protected.
• I will ensure that all sensitive data files sent via email are encrypted/password protected and the password sent via a separate message or over the phone.
• I will not store any sensitive personal documents, files or information on any school owned computer system.
• I will report any suspected data breaches/unauthorised sensitive data access to the school's Data Protection Lead.
• I will respect copyright and intellectual property rights.
• I will not attempt to bypass any filtering and/or security systems put in place by the school.
• I will report all suspected computer system damage, of virus or other malware to the ICT Systems Manager.
• I am responsible for all email, chat, sms blogs etc. that I post or send and will use language appropriate to the audience who may read them. I will be respectful in how I talk to and work with others online and never write or participate in online bullying. I will report any unpleasant material or messages sent to me. I understand my report will be confidential and may help to protect other students, staff and myself.

• I will not download or bring into school unauthorised programs, including games and videos and run them on school computers/equipment.
• I will not access inappropriate materials such as pornographic, racist or offensive material or use the school system for personal financial gain, gambling, political purposes or advertising.
• I understand that my use of the school information systems is logged.

APPENDIX 2

KING EDWARD VI ASTON SCHOOL

ACCEPTABLE USE AGREEMENT FOR SCHOOL WEBSITE AND VLE (MOODLE)

PARENTS AND CARERS

- The school website and Moodle are available to all parents/carers who have sons at the school. They are a means of parents/carers keeping up to date with school life and their son's progress.
- Access to the school website and Moodle are monitored using appropriate software.
- Every effort is made to filter out any inappropriate links from the school website but it must be realised that this is not always possible and therefore parents/carers should exercise caution when clicking on links to external sites.
- Parents and carers wishing to use the school website and Moodle must accept the following terms and conditions. Use of the website or accessing Moodle implies acceptance of these terms and conditions.

Terms and Conditions:

- All access to the school website should be appropriate to support your son at the school.
- The school reserves the right to examine or delete files or comments that are held on the school system.
- Access to Moodle should only be made using your allocated username and password. Any parents who have lost this should contact moodlesupport@keaston.bham.sch.uk.
- The username and password should not be made available to any other person.
- Any activity which threatens the integrity of the school's ICT system is forbidden.
- Copyright of all materials must be respected.
- Intentional misuse of the website or Moodle could result in access being withdrawn.
- Images of students may be used on the school's websites unless parents/carers have withdrawn permission when completing the annual SIMS permission form.

School Twitter Account @KEASTONVI:

The school runs a twitter account to keep parents and the wider community up to date with key information about school life. By following our twitter account, you are agreeing to these principles:

- The account is run by the school and is a professional account. No personal conversation will take place through the account.
- As a school, we will not follow any students or parents - the account is for providing updates about school life. Parents and students can continue to use the established means of communication with staff at the school.
- The school will not view the accounts of any parents or students who have chosen to follow us. The only exception to this is if the account is abused in any way, or if students receive inappropriate tweets following on from a post via the school's account

SHARP Reporting System

- The school website contains a link to the SHARP system. This system can be used by parents and students to alert the school anonymously about issues of concern with regard to keeping children safe online.

APPENDIX 3

USEFUL WEBSITES

Internet Watch Foundation Report inappropriate websites:	www.iwf.org.uk
UK COUNCIL FOR Child Internet Safety	https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
CEOP	https://ceop.police.uk/
THINKUKNOW	**https://www.thinkuknow.co.uk/**
UK Safer Internet Centre	https://www.saferinternet.org.uk/