HARBORNE
ACADEMY
ASPIRE.BELIEVE.ACHIEVE

Harborne Academy eSafety Policy

Policy Owner- Harborne Academy
Policy Author- Tina Dale
Governor approved – November 2014
Date of next review- October 2015

Contents

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Academy's need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Harborne Academy, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the Academy (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto Academy premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the Academy, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the Network Manager- to keep abreast of current issues and guidance through organisations such as Birmingham LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Headteacher / Network Manager and all Governors have an understanding of the issues and strategies at our Academy in relation to local and national guidelines and advice.

This policy, supported by the Academy's acceptable use agreements for staff, Governors, visitors and pupils is to protect the interests and safety of the whole Academy community. It is linked to the following mandatory Academy policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy**.**

eSafety skills development for staff

- Our staff receive regular information and training on eSafety issues in the form of staff meetings and briefings.
- New staff receive information on the Academy's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the Academy community.
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Managing the Academy eSafety messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each Academy year.
- E-safety posters will be prominently displayed.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The Academy provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating pupils on the dangers of technologies that maybe encountered outside Academy is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP make a report button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users agree to an Acceptable Use Agreement before they log in to the network, to demonstrate that they have understood the Academy's e-safety Policy.
- Users are provided with an individual network, email and Learning Platform log-in username. From Year 7 they are also expected to use a provided username and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the Academy network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the Network Manager or Technicians.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of Academy networks, CMIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- In the Academy, all ICT password policies are the responsibility of the network manager, and all staff and pupils are expected to comply with the policies at all times.

Data Security

The accessing and appropriate use of Academy data is something that the Academy takes very seriously

Staff are aware of their responsibility when accessing Academy data. Level of access is determined by the Headteacher.

- Data can only be accessed and used on Academy computers or laptops. Staff are aware they must not use their personal devices for accessing any Academy or pupil data

Managing the Internet Safely

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **Birmingham Metropolitan College** (BMET) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The Academy ensures that students will have supervised access to Internet resources (where reasonable) through the Academy's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute Academy software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- Birmingham Metropolitan College has a monitoring solution via Capita I.T. Services where web-based activity is monitored and recorded. This is monitored by the Network Manager on a weekly basis.
- Academy internet access is controlled through the Birmingham Metropolitan college web filtering service "Lightspeed" and a school internal filter called "policy central".
- Harborne Academy is aware of its responsibility when monitoring staff communication under current legislation.
- Staff and pupils are aware that Academy based email and internet activity can be monitored and explored further if required.
- The Academy uses management control tools (LanSchool) for controlling and monitoring workstations.

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Network Manager.
- It is the responsibility of the Academy, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all Academy machines.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the Academy's responsibility nor has the network manager to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it will be checked for viruses upon use in any academy computer through Microsoft endpoint removable device virus checker.
- Pupils and staff are not permitted to download programs or files on Academy based technologies without seeking prior permission from the Head teacher or Network Manager.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed.

Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the Academy endeavours to deny access to social networking sites to pupils within Academy.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, Academy details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the Academy.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the Learning Platform or other systems approved by the Headteacher.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of Academy too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in Academy is allowed. Our Academy chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The Academy allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the Academy allow a member of staff to contact a pupil or parent/ carer using their personal device.
- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The Academy is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the Academy community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the Academy community.
- Users bringing personal devices into Academy must ensure there is no inappropriate or illegal content on the device.

Academy provided Mobile devices (including phones)

- The sending of inappropriate text messages between any member of the Academy community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the Academy community.
- Where the Academy provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Where the Academy provides a laptop for staff, only this device may be used to conduct Academy business outside of Academy.

Managing email

The use of email within most of the Academy is an essential means of communication for both staff and pupils. In the context of Academy, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between Academy's on different projects, be they staff based or pupil based, within Academy or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- The Academy gives all staff their own email account to use for all Academy business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all Academy business.
- Under no circumstances should staff contact pupils, parents or conduct any Academy business using personal email addresses.

- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on Academy headed paper.
- Staff sending emails to external organisations, parents or pupils is advised to cc. the Headteacher, line manager or designated account.
- Pupils may only use Academy approved accounts on the Academy system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in Academy.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the Network manager/Head teacher if they receive an offensive e-mail.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the Academy community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the Academy permits the appropriate taking of images by staff and pupils with Academy equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the Academy's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the Academy's network and deleted from the pupils device.

Consent of adults who work at the Academy

- Permission to use images of all staff who work at the Academy is sought on induction and a copy is located in the personnel file

Publishing pupil's images and work

On a child's entry to the Academy, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the Academy web site
- on the Academy's Learning Platform
- in the Academy prospectus and other printed publications that the Academy may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the Academy's communal areas
- in display material that may be used in external areas, ie exhibition promoting the Academy
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this Academy unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.
Only the ICT Manager, having sought prior permission of the Headteacher, has authority to upload to the site.

- Images/ films of children are stored on the Academy's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the Academy network/ Learning Platform.
- The Network manager has the responsibility of deleting the images when they are no longer required, or the pupil has left the Academy.

Webcams and CCTV

- The Academy uses CCTV for security and safety. The only people with access to this are the Headteacher and site manager. Notification of CCTV use is displayed at the front of the Academy.
- We do not use publicly accessible webcams in Academy.
- Misuse of the webcam by any member of the Academy community will result in sanctions (as listed under the ' inappropriate materials' section of this document page 14)
  - CCTV can be found across the entire academy. Consent is sought from parents/carers and staff on joining the Academy, in the same way as for all images.

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the Academy.
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the Academy.
- Approval from the Head teacher is sought prior to all video conferences within Academy.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Misuses and Infringements

Complaints

Complaints relating to eSafety should be made to the Network manager or the Head teacher.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Network manager
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the network manager , depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct by staff meetings and regular e-safety discussions in lesson.

Equal Opportunities

Pupils with additional needs

The Academy endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the Academys' eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of Academy.   We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the Academy eSafety policy by initially contacting the Head teacher.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on Academy website)
- The Academy disseminates information to parents relating to eSafety where appropriate in the form of;
    - Information and celebration evenings
    - Posters
    - Website/ Learning Platform postings

- Newsletter items
- Learning platform training

Reviewing this Policy

Review Procedure

There will be an on-going opportunity for staff to discuss with the Network Manager any issue of eSafety that concerns them.

This policy will be reviewed every year and consideration given to the implications for future whole Academy development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

Human Rights Act 1998

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of Pupil's in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

All the acts above can be found at www.legislation.gov.uk