Harborne Academy Online Safety Policy

Policy Owner: Governing Body

Author: Sarah Ross

Approved By: Governing Body

Date of Review: September 2018

Date of Next Review: September 2019

Harborne Academy Online Safety Policy

1. Rationale

The Online-Safety Policy is part of the Academy's Development Plan. The policy has been written by the Academy, building on current Online-Safety policy guidelines and government guidance.

2. Teaching and Learning

2.1 Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The Academy has a duty to provide students with high-quality Internet access as part of their learning experience in school and prepare them to make safe and effective use out of school
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students

2.2 Internet use will enhance and extend learning

- The Academy Internet access will be designed expressly for student use and will include filtering appropriate to the age of students
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

2.3 Students will be taught how to evaluate Internet content

- Students will be educated that the use of Internet derived materials by staff and by students complies with Copyright Law and taught to be critically aware of the materials they read. They will be shown how to validate information before accepting its accuracy

3. Managing Internet Access Information System Security

- The Academy ICT system security will be reviewed regularly by the Network Manager
- Use of Policy Central is in place to monitor the use of the Internet
- The Network Manager will inform the DSL of any concerning Internet use in line with the Academy Safeguarding Policy
- Virus protection will be installed and updated regularly
- Security strategies will be discussed at least annually by the ICT Technician, Network Manager and Senior Leadership Team

4. E-mail

- Students may only use approved e-mail accounts on the Academy system
- Students will be taught to:
    - immediately tell a teacher if they receive an offensive e-mail

- not reveal their personal details or those of others, or arrange to meet anyone without specific permission
- treat incoming e-mail as suspicious and attachments not opened unless the author is known
- not forward on chain letters

5. Published content and the school web site

- Staff or student personal contact information will not generally be published. Any contact details given online should be those of the school office
- The Headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate

5. 1 Publishing students' images and work

- Photographs that include students will be selected carefully so that individual students cannot be identified or their image misused
- Students' full names will not be used anywhere on the Academy website or other on-line space, particularly in association with photographs
- Written permission from parents or carers is obtained when students join the Academy before photographs of students are published on the school website or in any other medium
- Work will only be published with the permission of the student and parents/carers

5.2 Social Networking and personal publishing

- The Academy will control access to social networking sites and consider how to educate students in their safe use. They will be blocked unless a specific use is approved
- Newsgroups will be blocked unless a specific use is approved
- Students will be given Online-Safety guidance on safe Internet use both in and out of school. This will include:
  - never to give out personal details of any kind which may identify them, their friends or their location
  - not to place personal photos on any social network space without considering how the photo could be used now or in the future
  - to only invite known friends and deny access to others when using social networking and instant messaging services
- Students will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications
- In line with the staff code of conduct, staff must not be 'friends' with students or ex-students on any social media website or application

6. Managing Filtering

- If staff or students discover an unsuitable site, it must be reported to the ICT Technician or the Network Manager

- The Network Manager and ICT Technician are responsible for ensuring that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

7. Managing Video-Conferencing

- In the Academy, video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet
- Students should ask permission from the supervising teacher before making or answering a video conference call
- Video conferencing will be appropriately supervised for the students' age

8. 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
- Technologies such as mobile 'phones with wireless Internet access may under some circumstances bypass school filtering systems and present a new route to undesirable material and communications. The Network Manager will do all that is reasonably practical to prevent this
- Mobile 'phones will not be used during lessons or formal school time, including break, lunchtime and before and after school on site. The sending of abusive or inappropriate text messages is forbidden
- The use by students of cameras in mobile 'phones will be kept under review
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location. They may only be used in the Academy with staff permission and supervision

9. Protecting Personal Data

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

10. Policy Decisions authorising Internet access

- All staff must read and sign the 'Acceptable use policy' before using any school ICT resource
- All staff are automatically prompted to ‘Agree’ to the policy when they use any school computer or laptop both on and off school site
- The Academy will maintain a current record of all staff and pupils who are granted access to Academy ICT systems
- Students must apply for internet access individually by agreeing to comply with the 'Acceptable use policy'
- Parents/carers will be asked to sign and return a consent form based on part of the 'Acceptable use policy'

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Academy network. The Academy cannot accept liability for any material accessed, or any consequences of internet access, although it will do all that is possible to reduce the risk of inappropriate material being accessed
- The Network Manager will monitor the network regularly to establish that the Online-Safety policy is adequate and that the implementation of the Online-Safety policy is appropriate and effective

11. Handling Online-Safety complaints

- Complaints of internet misuse will be referred to a member of the Senior Leadership Team
- Any complaint about staff misuse will be referred to the Headteacher
- Complaints of a child protection nature must be dealt with in accordance with the Academy safeguarding procedures
- Any cyber- bullying that occurs will be dealt with as any other bullying in accordance with the Culture for Learning Policy
- Malicious content may be reported to the Police or other Services

12. Communicating Online-Safety

12. 1 Introducing the Online-Safety Policy to students

- Online-Safety rules will be posted in all rooms where computers are used
- Students will be informed that network and Internet use will be monitored
- A programme of training in Online-Safety will be developed and delivered making use of appropriate materials, e.g. those from the Child Exploitation and Online Protection Centre (CEOP)

12. 2 Staff and the Online-Safety Policy

- All staff will be given a copy of the Academy's Online-Safety Policy and its importance explained
- Staff will be informed that network and internet traffic can be monitored and traced to the individual user
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues
- Staff should understand that telephone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship

12.3 Enlisting Parents' and Carers' support

- Parents' and carers' attention will be drawn to the Academy Online-Safety Policy in newsletters, the school brochure and on the school websites
- The Academy will maintain a list of Online-Safety resources for parents/carers

13. Policy Links

This Policy is linked to:

- The Safeguarding Policy
- Staff Code of Conduct
- Student Code of Conduct
- Culture for Leaning Policy

5. Policy documentation control

Responsible for review:	**Mrs Sarah Ross**
Version:	**1**
Reviewed:	**November 2017**
Next review date:	**November 2018**