E-Safety Policy

November 2016

RATIONALE

The e-Safety Policy is part of the Academy's Development Plan and relates to other policies including those for ICT Acceptable Use, Behaviour, Anti-bullying, Safeguarding and Child Protection, and Staff Behaviour – Code of Conduct.

BACKGROUND

The Policy was revised following consultation with the Principal and The Aspirations Academies Trust, the Local Area Board, the Academy Student Council and Magna staff.

1. Why the Internet and digital communications are important

1.1. 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

1.2. Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students

1.3. Internet use will enhance and extend learning

1.4. The Academy Internet access will be designed expressly for student use and will include filtering appropriate to the age of students

1.5. Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students

1.6. Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

1.7. Students will be taught how to evaluate Internet content

1.8. 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

2. Managing Internet Access Information System Security

2.1 Academy ICT system security will be reviewed regularly by the Network Manager

2.2 Virus protection will be installed and updated regularly

2.3 Security strategies will be discussed at least annually by the Network Manager and Senior Leadership Team

3. E-mail

3.1 Students may only use approved e-mail accounts on the school system

3.2 Students will be taught to: immediately tell a teacher if they receive offensive e-mail

3.3 Students will 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

4. Published content

4.1 Staff or student personal contact information will not generally be published. Any contact details given online should be those of the school office

4.2 The Principal or Designated Safeguarding Lead will take overall editorial responsibility and ensure that published content is accurate and appropriate

4.3 Photographs that include students will be selected carefully so that individual students cannot be identified or their image misused

4.4 Students' full names will not be used anywhere on a school website or other on-line space, particularly in association with photograph

4.5 Written permission from parents or carers is obtained when students join the Academy before photographs of students are published on the Academy website or in any other medium

4.6 Work will only be published with the permission of the student and parents/carers

5. Social Networking and personal publishing

5.1 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
5.2 Newsgroups will be blocked unless a specific use is approved
5.3 Students will be given e-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

6. Managing Filtering

6.1 The Academy will work in partnership with the South West Grid for Learning (SWGfL) to ensure that systems to protect students are reviewed and improved
6.2 If staff or students discover an unsuitable site, it must be reported to the Network Manager or Designated Safeguarding Lead
6.3 The Network Manager is responsible for ensuring that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

7. Managing Video-Conferencing

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

8. Managing Emerging Technologies

8.1 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
8.2 Technologies such as mobile 'phones with wireless Internet access may under some circumstances bypass the Academy 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
8.3 Mobile phones will not be used on the Academy site. The sending of abusive or inappropriate text messages is forbidden
8.4 The use by students of cameras in mobile 'phones is forbidden

9. Games machines

9.1 Microsoft Xbox, Sony PlayStation 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 school with staff permission and supervision

10. Protecting Personal Data

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

11. Policy Decisions authorising Internet access

11.1 All staff must read and sign the 'Acceptable use policy' before using any Academy ICT resource
11.2 The school will maintain a current record of all staff and pupils who are granted access to Academy ICT systems
11.3 Students must apply for internet access individually by agreeing to comply with the 'Acceptable use policy'
11.4 Parents/carers will be asked to sign and return a consent form based on part of the 'Acceptable use policy'
11.5 The Academy 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

11.6 The Network Manager will monitor the network regularly to establish that the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective

12. Handling e-safety complaints

12.1 Complaints of internet misuse will be referred to a member of the Senior Leadership Team
12.2 Any complaint about staff misuse will be referred to the Principal
12.3 Complaints of a child protection nature must be dealt with in accordance with the Academy child protection procedures

13. Communicating e-Safety

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

14. Staff and the e-Safety Policy

14.1 All staff will be given a copy of the Academy's e-safety Policy and its importance explained
14.2 Staff will be informed that network and internet traffic can be monitored and traced to the individual user
14.3 Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues
14.4 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

15. Enlisting Parents' and Carers' support

15.1 Parents' and carers' attention will be drawn to the Academy e-Safety Policy in Principal's Newsletters, the Academy prospectus and on the Academy website
15.2 The Academy will maintain a list of e-safety resources for parents/carers
15.3 The Academy will run e safety training sessions for parents/carers