AXE VALLEY ACADEMY

POLICY

Online Safety Policy

Updated: November 2017

Rationale

The policy has been written by the academy, building on current Online Safety Policy guidelines and government guidance.

Teaching and Learning

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 academy and prepare them to make safe and effective use beyond the confines of the academy.

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

Internet use will enhance and extend learning

- The academy internet access is designed expressly for staff and pupil use and will include filtering appropriate to the age of pupils.

- Clear boundaries are set for the appropriate use of the internet and digital communications and these are regularly discussed with staff and pupils.

- Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- Pupils will be educated that the use of internet derived materials by staff and by pupils 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.

Managing Internet Access Information system security

- Academy ICT system security will be reviewed regularly by the Senior Technician.

- Virus protection will be installed and updated regularly.

- Security strategies will be discussed at least annually by the Senior Technician and Senior Leadership Team.

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 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 chain letters.

Published content and the academy web site

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

Publishing students' images and work

- Photographs that include students will be selected carefully so that individual pupils 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 without parental consent.

- Written permission from parents or carers is obtained when students join the academy to allow photographs of students to be published on the academy website or in any other medium.

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

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 within and beyond the confines of the academy. This will include to:
  - 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.
  - 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.

Managing Filtering

- The academy will work in partnership with South West Gateway for Learning (SWGfL) to ensure that systems to protect pupils are reviewed and improved.

- If staff or students discover an unsuitable site, it must be reported to the Online Safety Coordinator or the Senior technician.

- The Senior technician and Online Safety coordinator are responsible for ensuring that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- The Senior technician and Online Safety coordinator are responsible for ensuring that the filtering methods are appropriate and effective in meeting any statutory duty, for example, The Prevent duty.

Managing Video-Conferencing

- In the academy IP videoconferencing will normally 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 videoconference call.

- Videoconferencing will be appropriately supervised for the students' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the academy is allowed.

- Technologies such as mobile phones with wireless internet access may under some circumstances bypass academy filtering systems and present a new route to undesirable material and communications. The Senior technician will do all that is reasonably practical to prevent this

- Mobile phones and devices that can connect to mobile phones will not be used during lessons or formal academy time for calls or messaging. The sending of abusive or inappropriate text messages is forbidden.

- The use by students of smartphones, tablets and cameras in mobile phones will be permitted where there is an identifiable educational benefit but only under staff supervision.

- 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 the academy or other officially sanctioned location. They may only be used in the academy with staff permission and supervision.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. This includes staff access to SIMS data at home.

Policy Decisions Authorising Internet access

- All staff must follow the 'staff acceptable use policy' whilst using any academy ICT resource.
- 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 'students' acceptable use policy'
- Parents/carers will be asked to sign and return a consent form based on the appropriate part of the students' acceptable use policy
- 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.
- The Senior technician 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.

Handling Online Safety complaints

- Complaints of Internet misuse will be referred to the Online Safety coordinator.
- Any complaint about staff misuse will be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with the acdemy child protection procedures.

Communicating Online Safety

Introducing the Online Safety policy to pupils

- 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 This will include addressing Online Safety issues with students in the Autumn Term of Year 7.

Staff and the Online Safety policy

- A member of the Senior Leadership team will be designated the Online Safety coordinator and they are the person responsible to the head teacher and governors for the day to day issues relating to online safety.

- All staff will be given the Academy 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 the Online Safety coordinator and work to clear procedures for reporting issues.

- Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

- Guidelines for the use of social media sites for educational purposes have been issued to staff along with those for 'safe working practices'.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the Academy Online Safety Policy in newsletters and on the academy website.

- The academy will maintain a list of Online Safety resources for parents/carers (see website).

Related Academy Policies
This Policy should be read in conjunction with the following documents:
Anti-Bullying Policy
Data Protection Policy
Mobile Phone Policy
Sex & Relationships Education Policy
Safeguarding Policy and Child Protection Policy
Preventing Radicalisation and British Values Policy