

INTERNET AND E-SAFETY POLICY

Writing and reviewing the e-safety policy

- The Academy will appoint an e-Safety coordinator. This will be the Designated Child Protection Coordinator.

Teaching and learning

Why Internet use is 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 quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The Academy's Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be 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

- The Academy will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Managing Internet Access

Information system security

- Academy ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

E-mail

- Pupils may only use approved e-mail accounts on the Academy system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain letters is not permitted.

Published content and the Academy web site

- The contact details on the Web site will be the Academy address, e-mail and telephone number.
- Staff or student personal contact information will not generally be published. The contact details given online should be the school office.

Publishing pupil's 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 a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- Work can only be published with the permission of the student and parents/carers.

Social networking and personal publishing

- The Academy will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Managing filtering

- The Academy will work in partnership with Kent, BECTA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager.

Managing videoconferencing

- IP videoconferencing should normally use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in Academy is allowed.
- The senior management team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- The Academy will maintain a current record of all staff and pupils who are granted access to Academy ICT systems.

Assessing risks

- The Academy will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a Academy computer. The Academy cannot accept liability for the material accessed, or any consequences of Internet access.
- The Academy will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Principal.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in networked rooms.
- Pupils will be informed that network and Internet use will be monitored.
- A programme of training in e-Safety will be developed, possibly based on the materials from CEOP.
- **Staff and the e-Safety policy**
- All staff will be given the Academy e-Safety Policy and its importance explained.

Enlisting parents' support

- Parents' attention will be drawn to the Academy e-Safety Policy in newsletters, the Academy brochure and on the Academy Web site.