UNIVERSITY ACADEMY OF ENGINEERING SOUTH BANK

Online Safety Policy

Introduction

Information Technology in the 21st Century is seen as an essential resource to support learning and teaching, as well as play an important role in the everyday lives of children, young people and adults. Consequently, the Academy needs to build in the use of these technologies in order to provide our students with the skills to access life-long learning and employment.

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 the University Academy of Engineering South Bank we understand the responsibility to educate our students in online safety; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet; technologies provided by the Academy; (such as PCs, laptops, webcams, whiteboards, digital video equipment, tablets etc.)

Aim

Online Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience; within the Academy or at home.

We have introduced the University Academy of Engineering South Bank's E-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

End to End Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all employees and students; encouraged by education and made explicit through published policies
- Sound implementation of Online Safety Policy in both administration and curriculum, including secure school network design and use

- Clear and structured procedures to deal with students and staff failing to comply with online safety guidelines
- Safe and secure broadband

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 students. The purpose of Internet use in the Academy is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the Academy's management functions.

Internet use will enhance learning

The Academy Internet access will be designed expressly for student use and will include filtering appropriate to the age of students. Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content

The Academy will ensure that the use of internet derived materials by employees and students complies with copyright law. Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students use the internet widely outside the Academy and will need to learn how to evaluate internet information and to take care of their own safety and security.

Information system security

- The Academy ICT systems capacity and security will be reviewed regularly
- Virus protection will be updated regularly
- Securus Software is used to protect students and staff on our curriculum network by way of notifying the safeguarding team of inappropriate and potential harmful behaviour
- Security strategies will be discussed regularly by the Senior Team
- Internet access will be planned to enrich and extend learning activities
- Access levels will be reviewed to reflect the curriculum requirements and age of students
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.

Password Security

- Adult users are provided with an individual network and email login, username and password, which they are encouraged to change periodically.
- All students are provided with an individual network, username and password.
- Students will be taught not to access on-line materials or files on the Academy network, belonging to their peers, teachers or others and that if they do find a way to access these they should inform their teacher immediately
- Staff will be aware of their individual responsibilities to protect the security and confidentiality of the Academy network, systems. This includes only the use of Academy USB storage devices, that are provided by the Academy

Email – Students will be taught that

- Email should be used for Academy related matters such as classwork, enrichment or home learning and if in doubt to check with a teacher
- The forwarding of chain letters is not permitted
- They may only use approved email accounts on the Academy system
- They should immediately tell a teacher if they receive offensive email. This can also be done through our safeguarding@uaesouthbank.org.uk
- They should not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission
- Any email to be sent to an external organisation by students or staff should be written carefully and authorised by the SLT before sending, in the same way as a letter written on Academy headed paper.

Social networking and personal publishing

- The Academy will filter access to social networking sites.
- The Academy will place an emphasis on educating the students to use social networking and personal publishing sensibly and within clear defined guidelines.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school attended and email address, full names of friends, specific interests and clubs etc.

Managing filtering

- The Academy will work with the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If employees or students discover an unsuitable site is accessible using the Academy Internet connection, it must be reported to a member of the SLT
- Senior leaders will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.

Protecting personal data

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

Authorising Internet access

- The Academy will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdraw.
- Families may be asked to sign and return a consent form.

Assessing risks

The Academy will take all reasonable precautions to ensure that users access only appropriate 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 an Academy computer. The Academy cannot accept liability for the material accessed, or any consequences of Internet access. The Academy will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a member of the senior team.
- Any complaint about staff misuse must be referred to the Principal
- Complaints of a child protection nature must be dealt with in accordance with Academy child protection procedures
- Students and parents or carers will be informed of the complaints procedure.

Community use of the Internet

The Academy will liaise with local organisations to establish a common approach to Online safety.

Introducing the online safety policy to Students

Online Safety protocols will be explained to students as they enrol into the Academy and discussed with the students at regular intervals. Students will be informed that network and Internet use will be monitored.

Online Safety skills development for staff

- Staff will receive regular information and training on online safety issues though lead

member of staff for online safety PD sessions

- Staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the Academy community. Report via safeguarding@uaesouthbank.org.uk
- All staff will incorporate online safety activities and awareness within their lessons and pastoral programme.

Online Safety information for families

- The Academy will send out relevant information through newsletters and the Academy website as appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully to avoid the potential for misuse of images.
- Students' full names will not be used anywhere on the Academy website in association with photographs.
- Written permission from families is obtained when a student joins the Academy for the use of photographs of students.

Monitoring and Evaluation

The CEO and the Principal will monitor the operation and effectiveness of the Academy's Online Safety policy.

References for Online Safety

CEOP (Childline Exploitation and Online Protection Centre): www.ceop.police.uk
ChildLine: www.childline.org.uk
Childnet: www.childnet.com
Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk
Cybermentors: www.cybermentors.org.uk
Digizen: www.digizen.org.uk
Internet Watch Foundation (IWF): www.iwf.org.uk
Kidsmart: www.kidsmart.org.uk **Teach Today**: http://en.teachtoday.eu
Think U Know website: www.thinkuknow.co.uk
Virtual Global Taskforce – Report Abuse: www.virtualglobaltaskforce.com