

# Furness Academy: E-Safety Policy

This E-safety Policy relates to other policies including those for Safeguarding, anti bullying and child protection.

The Academy designated Child Protection Team is composed of:

- Pauline Hughes= Academy Designated Child Protection Teacher
- Deb Warbrick - South Site designated CP Teacher
- Chris Ashurst - North Site designated CP Teacher

E-Safety overlaps with this role but it is not a technical role.

Our E-Safety Policy has been written by building on the CLEO e-Safety and government guidance.

## E-Safety

'E-safety', and related terms such as 'online', 'communication technologies', and 'digital technologies' refer to all fixed and mobile technologies that children may encounter, now and in the future, which might pose e-safety risks.

The Byron Review classifies e-safety risks as involving **content**, **contact** and **conduct**, illustrating that the risk element involved in using new technologies is often determined by **behaviours** rather than the technologies themselves. A student may be a recipient, participant or actor in online activities posing risk.

## Teaching and learning

### Why the Internet and digital communications are important

Internet use will enhance learning. 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.

As detailed in the document 'Furness Academy: ICT Vision', ICT will be used across the Academy to enhance and extend learning, to engage in interesting and vibrant learning activities and to empower learners so that they play a more active role in managing their own learning experiences. Through the use of the VLE, and Internet video and audio communications, learning facilities will be extended to the home and other environments for all learners.

### Safe and appropriate internet use

The Academy Internet access will be designed expressly for student and staff 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. In line with the National Curriculum, Every Child Matters, Functional Skills requirements and BECTA advice, the Academy's aim will be to educate pupils in how to keep safe when using the internet both at home and at school. Such education will focus on what constitutes E-safety, current digital communication threats and cyber-bullying.

There will be regular audits of protocols and the management of E-safety and the implementation of E-safety will be regularly reviewed to keep pace with Internet developments. The Academy will use Becta's 'Self-Review Framework' to drive continual improvement of our use of ICT including E-safety.

The Academy's AUP (Acceptable use Policy) will be regularly reviewed, monitored and agreed with parents, students and staff.

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 shown how to safely and effectively publish and present information to a wider audience.

### **Students will be taught how to evaluate Internet content**

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

Students will be taught the importance of cross-checking information before accepting its accuracy.

Students will be taught how to report unpleasant and/or unacceptable Internet content to a member of staff.

## **Managing Internet Access**

### **Information system security**

Academy ICT systems security will be reviewed regularly.

Virus protection will be updated regularly.

Security strategies will be discussed with the Local Authority (CLEO) where applicable.

### **E-mail**

Students may only use approved e-mail accounts on the Academy system.

Students must immediately tell a teacher if they receive offensive e-mail.

Students will be educated to be aware that, in e-mail communication, they must not reveal their personal details or those of others, or arrange to meet anyone without specific permission from their parents or Academy staff members.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The Academy will consider how e-mail from students to external bodies is presented and controlled.

The forwarding of chain letters is not permitted.

**Published content and the Academy web site**

Staff or student personal contact information will not be published. The contact details given online will be the Academy office.

The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

**Publishing Students' images and work**

Photographs that include students will be selected carefully so that individual students cannot be identified or their image misused. The Academy will consider using group photographs rather than full-face photos of individual children.

Written permission from parents or carers will be obtained before photographs of students are published on the Academy Web site.

Students' full names will not be used anywhere on an Academy Web site or other on-line space, particularly in association with photographs.

Pupil image file names will not refer to the pupil by name.

Parents will be clearly informed of the Academy policy on image taking and publishing, both on Academy and independent electronic repositories. (Children, Families, Health and Education Directorate page 6 June 2008)

**Social networking and personal publishing**

The Academy will control access to social networking sites, and will educate students in their safe use.

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, their friends or their location.

Ideally students would use only moderated social networking sites, e.g. SuperClubs Plus and the Academy's own VLE forums.

Students and parents will be advised that the use of social network spaces outside Academy brings a range of dangers for students.

Students will be advised to use nicknames and avatars when using social networking sites.

The Academy will respond sensitively and effectively to cyber-bullying which may occur on social networking sites; the Academy is aware that staff, as well as students, can be victims of harassment/bullying/intimidation via such sites.

**Managing filtering**

The Academy will work with the providers to ensure systems to protect students are reviewed and regularly improved.

If staff or students discover unsuitable on-line materials, the site must be reported to the class teacher and Network Manager.

The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### **Managing videoconferencing and webcam use**

Videoconferencing should use the educational broadband network to ensure quality of service and security.

Students must ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing and webcam use 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.

The senior leadership team are aware that technologies such as mobile phones with wireless Internet access can bypass Academy filtering systems and present a new route to undesirable material and communications.

Mobile phones will not be used during lessons unless at the direction of a class teacher for a suitable educational and relevant purpose as part of a lesson plan. The use by students of cameras in mobile phones will be kept under review.

The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

Games machines including the Sony Playstation, Microsoft Xbox, Nintendo Wii and others have Internet access which may not include filtering. Care is required in any use in Academy or other officially sanctioned location.

Staff may be issued with an Academy phone where contact with students is required or where mobile phones are used to capture photographs of students. (Children, Families, Health and Education Directorate page 7 June 2008)

The appropriate use of both open and closed Learning Platforms will be discussed as the technology becomes available within the Academy.

### **Protecting personal data**

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

### **Authorising Internet access**

All staff must read and sign the 'Acceptable User Agreement' before using any Academy ICT resource.

The Academy will maintain a current record of all staff and students who are granted access to Academy ICT systems.

All students must read and sign the 'Acceptable User Agreement' before using any Academy ICT resource, which will also be countersigned for consent by parents.

Any person not directly employed by the Academy will be asked to sign an 'Acceptable User agreement' before being allowed to access the ICT resources and internet from the Academy site.

**Assessing risks**

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.

The Academy will regularly audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

**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.

Complaints of a child protection nature must be dealt with in accordance with Academy child protection procedures.

Students and parents will be informed of the complaints procedure (see Academy's complaints policy)

Students and parents will be informed of consequences for students misusing the Internet, which can include the loss of internet access temporarily or permanently.

'Acceptable Use Rules for Staff' and 'Acceptable Use Rules for Students' are separate documents available from the Academy's ICT Services.

**Sept 2010**