

# Darwen Aldridge Community Academy



THE  
ALDRIDGE  
FOUNDATION

The sponsor is keen to ensure that our students have the latest technologies at their disposal, but is aware of the safety implications that come with this and this policy ensures that the safety of our children is paramount.

# Darwen Aldridge Community 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 Officer is Mr David Cane. Any concerns over e-safety should be directed to him in the first instance. If he is unavailable, then please speak to Mrs Fiona Beaumont (deputy designated child protection officer) or Mr Brendan Loughran (Principal).

If you wish to seek further advice, please go to the following link: [www.blackburn.gov.uk](http://www.blackburn.gov.uk). Here you will find the policies and procedures for the Local Safeguarding Children's Board (LSCB) Our Local Authority Designated Officer is Robina Jillhani who can be contacted on 01254 587547.

## 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 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.

### **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 shown how to 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 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 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.

In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission. 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 should be the Academy office. The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

### **Publishing Student's 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. Signed permission from parents or carers will be obtained before photographs of students are published.

Students' full names will not be used anywhere on the 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 should 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 not allow access to social networking sites, and uses assemblies and tutorials to educate students in their safe use outside of the Academy building. The DCPO will advise parents on how to keep their children safe online during Parent Forum and by letter. Students will be advised never to give out personal details of any kind which may identify them, their friends or their location. Students and parents will be advised that the use of social network spaces outside the Academy brings a range of dangers for students.

### **Managing filtering**

The Academy will work with the providers to ensure systems to protect students are reviewed and improved. If staff or students come across unsuitable on-line materials, the site must be reported to the class teacher who needs to inform the DCPO and the 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 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 and must be switched off. Staff may be issued with a Academy phone where contact with students is required but must have their personal mobile phones switched off during the Academy day.

The appropriate use of 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 should 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. This should be done annually.

### **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. (Inform the DCPO using the appropriate cause for concern sheet.) Students and parents will be informed of consequences for students misusing the Internet, which can include the loss of internet access

temporarily or permanently. The Acceptable User Agreement' is separate document available online or a hard copy can be obtained from Student Services, within the Academy.

November 2009