eSafety Policy

Policy/Procedure Reference Number	089
Author / Role	J McKay, COO
Date prepared	1.9.18
Adopted by Board	Sep 18
Implementation Date	September 2018
Review Date	July 2019
Version Control	002
Status	Best practice
Senior Manager Authoriser	Principals

Contents

Principles

The University of Chester Academies Trust (UCAT) believes that the use of information and communication technologies brings great benefits. The Trust recognises the e-Safety issues and this policy will ensure appropriate, effective and safe use of electronic communications.

The Trust e-Safety policy encompasses internet technologies and electronic communications such as mobile phones and wireless technology. The Trust e-Safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Anti-Bullying, Curriculum, ICT Acceptable Use, Safeguarding, Social Media and Data Protection.

Thorough eSafety

e-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-Safety policy in both administration and curriculum, including secure academy network design and use.
- Safe and secure broadband.
- National Education Network standards and specifications.

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 Trust has a duty to provide pupils 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 Trust 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 to Evaluate Internet Content

The Trust will ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information System Security

Trust ICT systems capacity and security will be reviewed regularly.

Virus protection will be installed and updated regularly

eMail

Pupils may only use approved e-mail accounts on the Trust 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.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on academy headed paper.

The forwarding of chain letters is not permitted.

Published Content and Trust and Academy Websites

The contact details on Trust web sites will be academy addresses, e-mails and telephone numbers. Staff or pupils' personal information will not be published.

The Principal (or nominee) will take overall editorial responsibility and ensure that content is accurate and appropriate in each academy.

Publishing Pupils' Images and Work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on any Trust web site or blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on any Trust web site.

Work will only be published with the permission of the pupil and parents.

Social Networking and Personal Publishing

The Trust 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 must not place personal photos on any social network space.

Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and know how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others.

Managing Filtering

The Trust will work in partnership with 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 Co-ordinator or the Network Manager in their academy.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Video Conferencing

Video conferencing should use the educational broadband network to ensure quality of service and security rather than the internet.

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

Video conferencing will be appropriately supervised for the pupils' age group.

Managing Emerging Technologies

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

Mobile 'phones will not be used during lessons or formal academy time.

The sending of abusive or inappropriate text messages is forbidden.

Staff will be issued with an academy phone where contact with pupils is required.

Protecting Personal Data

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

Authorisation

All staff must read and sign the 'ICT Acceptable Use' form before using any academy ICT resource.

Each academy will maintain a current record of all staff and pupils who are granted access to academy ICT systems.

Pupils must apply for internet access individually by agreeing to comply with the ICT Acceptable Use statement.

Parents will be asked to sign and return a consent form.

Assessing Risks

The Trust 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 Trust computer. The Trust cannot accept liability for the material accessed, or any consequences of internet access.

The Trust 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 eSafety 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 Trust Safeguarding Policy.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

e-Safety rules will be posted in all networked rooms.

Pupils will be informed that network and internet use will be monitored.

Staff, Trustees and SOAC Members

All staff will be given the Trust's e-Safety Policy and its importance explained.

Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Parents

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

Monitoring, Evaluation and Review

The Board will review this policy at least every two years and assess its implementation and effectiveness through the Chief Operating Officer. The policy will be promoted and implemented throughout the Trust.