Community First
Academy Trust

E-Safety Policy

Community First Academy Trust
Rivington Avenue, Platt Bridge, Wigan WN2 5NG
T. 01942 487973 | **E.** info@cfat.org.uk
www.cfat.org.uk

ADOPTED AT THE MEETING OF THE LOCAL ACADEMY BOARD

CHAIR OF BOARD: Mr M Farrell

Date: September 2018

Planned Review Date: September 2020

Effective Practice in E-Safety

E-Safety depends on effective practice in each of the following areas:

Education for responsible ICT use by staff and pupils.
A comprehensive, agreed and implemented e-Safety Policy.
A school network that complies with the National Education Network standards and specification.

1. Writing and reviewing the e-safety policy

Our e-Safety Policy has been written and been agreed by senior management and approved by governors.

2. Teaching and learning

2.1 Why the Internet and digital communications are important

The Internet is an essential element in modern life for education, business and social interaction.
The school has a duty to provide pupils with quality internet access as part of their learning experiences, enriching their learning to holistically develop the 21st century child.
Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, allowing co-operation, communication and collaboration.

2.2 Internet use will enhance learning

The school 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.

2.3 Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
Pupils will be taught the importance of cross-checking information before accepting its accuracy and reliability, using safe search techniques.
Pupils will be taught how to report unpleasant Internet content by informing a member of staff (in school) or parent/carer (at home) and they will be familiar with the CEOP Report Abuse icon (at age appropriateness).

3. Managing Internet Access

3.1 Information system security

School ICT systems security will be reviewed regularly.
Virus protection will be updated regularly
Security strategies will be discussed with the Local Authority and ICT infrastructure contractor.

3.2 E-mail

Pupils may only use approved e-mail accounts on the school system, emailing staff or their peers.
Pupils must immediately tell a teacher if they receive offensive e-mail.

In e-mail communication, pupils 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 from peers or authorised staff members.

3.3 Published content and the school web site

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

3.4 Publishing pupil's images and work

Pupils' full names will not be used on the school web site or other on-line space (blogs, etc.), in association with photographs.
Pupils' full names may appear in sports or other activity reports, however written permission from parents or carers will be obtained before publication.
Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

3.5 Social networking and personal publishing

The school will control access to social networking sites, and consider how to educate pupils in their safe use using discrete e-safety lessons to deliver information about Facebook/Twitter usage, including cyber-bullying issues.
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, their friends or their location whilst online in any capacity.
Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
Pupils will be advised to use nicknames and avatars when/if using social networking sites.

3.6 Managing filtering

The school will work with partners to ensure systems to protect pupils are reviewed and improved.
If staff or pupils come across unsuitable on-line materials, the site must be reported to the ICT Coordinator and recorded with date and time.
Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7 Managing video conferencing & webcam use

Videoconferencing should use the educational broadband network to ensure quality of service and security through appropriate filtering.
Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

3.8 Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed either by the ICT coordinator or a member of SLT.
The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school through appropriate training/dissemination of the information.

3.9 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 2018.

4 Policy Decisions

4.1 Authorising Internet access

All staff must read and sign the ‘LEA Internet and Email’ policy before using any school ICT resources.
The school will maintain a record of all staff and pupils who are granted access to school ICT systems.
At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
Parents will be asked to sign and return a consent form.

4.2. Assessing risks

The school 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 school network. Neither the school nor Wigan Council can accept liability for any material accessed, or any consequences of Internet access.
The school will 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 through monitoring and questionnaires to assess staff habits in school.

4.3. 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 Head of School who, depending on the nature of the complaint may refer to the LADO.
Complaints of a child protection nature must be dealt with in accordance with school procedures.
Pupils and parents will be informed of the complaints procedure.
Pupils and parents will be informed of consequences for pupils misusing the Internet.

4.4. Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.

5 Communications Policy

5.1. Introducing the e-safety policy to pupils

E-Safety rules will be posted and displayed within the classroom behind computers and discussed with pupils regularly when using ICT.
Pupils will be informed that network and Internet use will be monitored and appropriately followed up if misused.
E-Safety training will be embedded within the ICT scheme of work and the Personal Social and Health Education (PSHE) curriculum

5.2. Staff and the e-Safety Policy

All staff will be given the School e-Safety Policy and its importance explained.
Staff will be informed that network and Internet traffic can be monitored and traced to the individual user. Records are also archived for a six year period.
Staff will always use a child friendly safe search engine when accessing the web with pupils.

5.3. Enlisting parents’ and carers’ support

The school will ask all new parents to sign the parent/pupil agreements of acceptable ICT usage when they register their child with the school.

6 Monitoring and review

6.1 This policy is monitored by the Local Governing Body, and will be reviewed every two years, or earlier if necessary.

Signed:

Date: