St Clere's
Co-operative Academy Trust

Policy/Procedure	**e-Safety Policy**

First approved by Trust Board: March 2013

Review frequency: Annual

Date of last review: March 2016

Date of next review: March 2017

St Clere's Co-operative Academy Trust is a multi-academy trust (MAT) incorporated around the principles and values of the international co-operative movement. These are Equality, Equity, Democracy, Self-help, Self-Responsibility and Solidarity, along with the ethical values of openness, honesty, social responsibility and caring for others. These values and principles underpin all our actions.

Introduction

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 Trust network design and use;
- Safe and secure broadband;
- National Education Network standards and specifications.

E-safety encompasses all aspects of school life and includes:

- **Teaching and learning**
- **Managing ICT Systems**
- **ICT related Policies**
- **Communications Policy**

Teaching and Learning

Why internet use is important

- The internet is an essential element in 21st century life for education, business and social interaction. St Clere's Co-operative Academy 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.
- The purpose of Internet use in the Trust is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Benefits of using the Internet in education include:
  - access to worldwide educational resources including museums and art galleries;
  - inclusion in the National Education Network which connects all UK schools;
  - educational and cultural exchanges between pupils worldwide;
  - access to experts in many fields for pupils and staff;
  - professional development for staff through access to national developments, educational materials and effective curriculum practice;
  - collaboration across networks of schools, support services and professional associations;
  - access to learning wherever and whenever convenient.

Internet use will enhance learning

- The Trust's internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children.
- 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 acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Pupils will be taught how 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 will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.

Managing ICT Systems

Information system security

- The Trust's ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the appropriate authorities.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.

E-mail

- 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 the Trust or School headed paper.
- The forwarding of chain letters is not permitted.
- Staff should not use personal email accounts during school hours or for professional purposes.

Published content and the Trust and School web sites

- The contact details on the web sites will be the address, e-mail and telephone number. Staff or Pupils personal information will not be published.
- The Headteacher (or nominee) from each school will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Trust and school websites will respect intellectual property rights, privacy policies and copyright.

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 the web sites or in blogs, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the Trust or schools' web sites.
- Work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The Trust and the schools will control 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 should be advised on security and encouraged to set passwords, deny access to unknown individuals and know how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Staff official blogs or wikis should be password protected and run from the schools' websites with approval from the Head Teacher or CEO.

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, Network Manager or Headteacher.
- Any material that the Trust or its schools believes is illegal will be reported to appropriate agencies such as IWF, the Police or CEOP.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Video conferencing will use high-end and low-end videoconferencing solutions and will favour the educational broadband network to ensure quality of service and security rather than the internet.
- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the pupils' age group.

- Trust or schools' video conferencing equipment will not be taken off school premises without permission.

Managing emerging technologies

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

- Mobile phones / Smartphones will not be used during lessons or formal school time unless approved by the school. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the
Data Protection Act 1998. A Trust Data Handling Policy has been created.

Policy Decisions

Authorising internet access

All staff must read and sign the 'Responsible use of ICT' Acceptable Use Policy (ACP) form before using any school ICT resource.

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

- Pupils must apply for internet access individually by agreeing to comply with the Responsible Internet Use statement.
- Parents will be asked to sign and return an AUP consent form.

Assessing risks

The Trust and the schools 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 school's 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 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 school's Head Teacher or the Trust CEO.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- All members of the Trust community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the Trust community.

Community use of ICT

The Trust will provide an AUP for any guest who needs to access the Academy computer system or internet on site.

Guests will have to abide by guidance within the e-Safety policy.

Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- The Trust will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the Trust to support the approach to cyberbullying and the schools' e-Safety ethos.

Learning Platform

The Senior Leadership Team (SLT) and staff will regularly monitor the usage of the Learning Platform (LP) by pupils and staff in all areas, in particular message and communication tools and publishing facilities.

- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.

Mobile devices and personal devices

The use of mobile phones and personal devices in the Trust will be decided on an individual basis.

- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- Electronic devices of all kinds that are brought into the Trust or one of its schools are the responsibility of the user. The trust accepts no responsibility for the loss, theft or damage of such items. Nor will the Trust accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.

Communications Policy

Introducing the e-Safety policy to pupils

- E-Safety rules will be posted in all networked rooms.
- Pupils will be informed that network and internet use will be monitored.

Staff and the e-Safety policy

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.
- The Trust will highlight useful online tools, which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.

Enlisting parents' support

Parents' attention will be drawn to the Trust's e-Safety Policy in newsletters, the schools' prospectus and on the Trust and school web site.

Monitoring, Evaluation and Review

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