Cabot
Learning
Federation

E-Safety Policy

Date Adopted: November 30th 2017
Cabot Learning Federation
Implementation Date: January 2018

History of most recent Policy changes

Date	Page	Change	Origin of Change e.g. TU request, Change in legislation
Date	E.g. Whole Document	Detail of change	Reason for change

Contents

History of most recent Policy changes 2

Contents 3

1 Introduction 4

2 Approach 4

3 Filters 5

4 Monitoring 5

5 Training and resources 6

6. Useful Websites 7

Appendix One 8

1. Introduction

The Cabot Learning Federation enables students, teachers and co-professionals access to network services and the Internet. All network activity and Internet access in the Academy must be in support of education, research or business operations, and must be appropriate to the educational objective of the Cabot Learning Federation. It is important that all network users are aware that systems are in place to track and record what is happening across the structured cabled network and wireless cloud.

This policy applies to all members of the Cabot Learning Federation community (including staff, students, volunteers, parents, visitors and community users) who have been granted a user account or access to Cabot Learning Federation ICT systems, both in and out of Academy and by remote connection.

Anyone who is aware of any type of E-Safety issue that is taking place is expected and has a duty to inform a Designated Safeguarding Lead immediately.

This policy should be considered in conjunction with the Safeguarding and Child Protection Policy which outlines the Cabot Learning Federation procedures for safeguarding children as well as the Prevent Duty Guidance for England and Wales (2015)

2. Approach

New technologies have become integral to the lives of children and young people in today's society, both within their academic lives and also in their lives away from academia. We want young people to be able to fully exploit the benefits offered by ICT while doing so in a safe manner.

Online messaging, social networking and mobile technology effectively mean that children can always be 'online'. Their social lives, and therefore their emotional development, are bound up in the use of these technologies. Latest e-safety guidance states that the breadth of e-safety issues can be categorised into three areas of risk:

1. **content**: being exposed to illegal, inappropriate or harmful material
2. **contact**: being subjected to harmful online interaction with other users
3. **conduct**: personal online behaviour that increases the likelihood of, or causes, harm.

The purpose of this policy is to ensure that Cabot Learning Federation Academies are kept aware of the risks as well as the benefits of technology and how to manage these risks and keep themselves and others safe. It details the measures that the school have put in place to support this as well as the rules and restrictions around the use of ICT and other technology across the Cabot Learning Federation.

3. Filters

All Cabot Learning Federation internet connections are subject to internet access controls. These controls restrict the type of internet connections that can be established.

By default general web traffic (HTTP and HTTPS) is permitted. Other types of connections will be subject to review.

All web traffic is filtered as defined by filter categories in addition to whitelists and blacklists to supplement the categories where required. The filter categories must be regularly updated and include blacklists as defined by the Internet Watch Foundation.

Whilst every effort will be made to ensure inappropriate content is not accessible, the CLF recognise that some inappropriate access could still be possible. The CLF mitigates against the impact of this gap through appropriate education of all users, and additional safety mechanisms, such as computer monitoring software.

4. Monitoring

All connections to the internet are monitored. Where possible capturing the username, date, time and URL that is accessed. All academies use Impero to monitor internet usage.

To monitor and provide enhanced filtering of the internet the CLF will intercept and decrypt HTTPS traffic. Traffic relating to financial services and health and medicine categories will not be intercepted.

Where possible computer workstations will have additional monitoring software installed. This software will also:

- monitor sites accessed on the internet;
- monitor applications used on the computer;
- capture keystrokes, alerting appropriate staff to specific keywords that are typed;
- provide remote monitoring and control of computers for use by teachers and ICT services.

All CLF computers are protected by a number of different mechanisms to keep the computers and all users safe. These protections will include:

- specific policies to limit the administrative access of the device;
- firewalls and anti-virus software to protect against malicious attack of the device;
- regular software update processes to automatically patch vulnerabilities.

5. Training and resources

a. Education of Pupils and the Curriculum

The most important aspect of keeping young people safe online is education. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience, and to ensure that they are not at risk when they are outside of the safe environment provided at school.

- We have an age-related e-safety curriculum that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm, understand how to manage risk, how to take responsibility for their own and others safety and how to be responsible users of technology.
- Key e-safety messages are reinforced through assemblies.
- Acceptable use of the school's ICT systems is discussed with pupils in every class and all classes discuss their rules for e-safety which are displayed in classrooms, student planners and in all computer suites.
- Students are given age appropriate support to search safely and to evaluate the content that they access online. Processes are in place for dealing with any unsuitable material that is found in internet searches. Staff are vigilant in monitoring the content of the websites the young people visit and encourage students to use specific search terms to reduce the likelihood of coming across unsuitable material.
- Students are taught to be critically aware of the materials / content they access online and be guided to validate the accuracy of information. Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Our behaviour policy is also used to reinforce online behaviour with appropriate sanctions for irresponsible use.
- Older pupils are involved in providing support for younger ones through working on activities with them and presenting in assemblies.
- Staff share with pupils how to deal with issues outside school where there may be no filtering
- Teachers monitor ICT use during lessons, including the use of Impero, to monitor student screens.
- It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the CLF's E-safety Policy and Acceptable Use Agreements (See Appendix One).
- All staff will receive annual "refresher" training in e-safety as part of their annual safeguarding briefing which will include Impero

b. Education & Training – Parents /carers

Parents and carers may have only a limited understanding of e-safety issues and may be unaware of risks and what to do about them. They have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The school supports parents to do this by:

- Providing clear acceptable use guidance which can found on academy websites. All websites have translation facilities to support parents who have English as an additional language
- Providing a regular awareness raising e-safety sessions for parents / carers
- Parents and carers may have only a limited understanding of e-safety issues and may be unaware of risks and what to do about them. They have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences.

The school supports parents to do this by:

- Providing clear acceptable use guidance
- Providing information and guidance on all academy websites, Parents and carers will be regularly updated in line with any legislation changes

c. Education and Training – Staff and Governors

There is a planned programme of e-safety training for all staff and relevant governors to ensure they understand their responsibilities, as outlined in this policy.

- All Staff receive e-safety training and it is included in the induction program for new staff
- Members of the e-Safety working group receive regular updates through attending a variety of e-Safety training events and conferences.
- This E-Safety policy and acceptable use are discussed in staff meetings.
- The Director of ICT provides advice/guidance and training as required
- Staff act as good role models for students in their own use of ICT
- Academy Councillors are invited to be included in e-safety awareness sessions and training.

6. Useful Websites:

http://www.thinkyouknow.co.uk/

http://www.safetynetkids.org.uk/

http://kidsmart.org.uk/

https://www.nspcc.org.uk/

http://www.ltai.info/what-is-prevent/

Keeping children safe documentation