DRAFT – AWAITING ACADEMY COUNCIL APPROVAL

Cabot Learning Federation

CLF Online Safety Policy

Cabot Learning Federation
Date Adopted: March 2022 Cabot Learning Federation
Implementation Date: March 2024

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
V1.0 Jan 2020	Whole documents	Drafted policy	Adoption by the Cabot Learning Federation and Implementation
V2.0 March 2021	Whole document	Reviewed in line with Remote Education Policy – minor changes	Pandemic adaptations to policy structure
V2.1 July 2021	**Minor change**	**Updated to reflect Senso monitoring**	**Change in monitoring system – Senso – policy to reflect the filtering system**
V2.2 March 2022	**Full review**	**Annual review**	**Equalities Impact Assessment carried out**
V2.3 March 2023	**Update**	**Annual Review**	**Check changes and confirm EQIA – headline assessment – with full further assessments to follow in line with 2024 Annual update and EDI developments.**
V2.4 March 2024	**Update**	**Annual Review**	**EQIA process in development.** **Policy to be released and reviewed 2024-25.**

Cabot Learning Federation

Contents

1. Aims 4

2. Legislation and guidance 4

3. Roles and responsibilities 4

4. Educating pupils about online safety 6

5. Educating parents about online safety 7

6. Cyber-bullying 7

7. Acceptable use of the internet in school 8

8. Pupils using mobile devices in school 8

9. Staff using work devices outside school 8

10. How the school will respond to issues of misuse 9

11. Training 9

12. Monitoring arrangements 9

13. Links with other policies 10

Appendix 1: acceptable use agreement (pupils and parents/carers) 11

1. Aims

The Cabot Learning Federation aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and across our governance structures
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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 utilise 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 schools 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. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

4. Roles and responsibilities

4.1 The Trust Board and Academy Council

The Trust board have overall responsibility for monitoring this policy and ensuring the systems are in place for holding the Principals to account for its implementation.

The Principal/SLT/ Online Safety Lead will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Academy Councillor who oversees online safety is Kerry Francis

All Academy Council/Board members will:

- Ensure that they know the policy is in place and understand how the policy is managed at Academy Level.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

4.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) are set out in the Cabot Learning Federation Safeguarding Policy.

The DSL takes lead responsibility for online safety in school, in some cases alongside an Online Safety Lead and the Safeguarding team in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Linking with the Academy Online Safety Lead, where this is another member of the team
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

4.4 IT Director

CLF Head of IT is responsible for:

- Working across the Cabot Learning Federation to ensure that appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at the Academy, including terrorist and extremist material
- Ensuring that all security aspects relating to IT that the CLF manage including Antivirus/Windows updates/Backups are monitored and/or updated within a reasonable timescale of their general release availability.

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are monitored and logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy Safeguarding policies

4.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the Academies ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy

This list is not intended to be exhaustive.

4.6 Parents/Carers

Parents/Carers are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Understand that their child, in using Academy ICT systems, will have read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

4.7 Visitors and members of the community

Visitors and members of the community who use the Academies IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1).

5. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

6. Educating parents/carers about online safety

The academy will raise parents'/carers' awareness of internet safety in letters or other communications home, in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents'/carers' evenings/workshops.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

7. Cyber-bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, Academy Council members and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training

The academy also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy will use all reasonable endeavors to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the academy rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of academy discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the academy complaints procedure.

8. Acceptable use of the internet in the Academy

All pupils, parents, staff, volunteers and governors are made aware of the Acceptable Use agreement regarding the acceptable use of the academy's ICT systems and the internet. Visitors will be expected to read and agree to the academy's terms on acceptable use if relevant.

Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements which are adapted through guidance to be age-appropriate and appears as pop up for users to accept before log-in on sites where this additional feature has been enabled locally.

9. Pupils using mobile devices in the Academy

Adapt this section to reflect your Academy approach.

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Break and lunch times
- Tutor group time
- Clubs before or after school, or any other activities organised by the academy

Any use of mobile devices in school by pupils must be in line with the terms of acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the academy behaviour policy, which may result in the confiscation of their device.

10. Staff using work devices outside of the Academy

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the academy's terms of acceptable use, as set out in the CLF Data Protection Policy, CLF Acceptable Use of Equipment, The CLF Information Security Policy and Code of Conduct.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the academy must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

11. How the Academy will respond to issues of misuse

Where a pupil misuses the academy's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the academy's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL will undertake child protection and safeguarding training and all staff are required to complete an online Safeguarding suite of courses via Nimble, which will include elements of online safety. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Academy Councillors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. 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 cleared lists and barred lists 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.

Filtering and monitoring

The updated guidance makes it clear that all staff should receive training on the expectations, applicable roles and responsibilities in relation to filtering and monitoring. The designated safeguarding lead should take lead responsibility for understanding the filtering and monitoring systems and processes in place. Information on school child protection policies should include information on appropriate filtering and monitoring on school devices and school networks. The guidance signposts the Department for Education's new filtering and monitoring standards (DfE, 2023b), which support schools to have effective systems in place. Schools and colleges should consider meeting the DfE's Cyber security standards for schools and colleges (DfE, 2023c).

Additions to the guidance state that governing bodies and proprietors should regularly review the effectiveness of school filters and monitoring systems. They should ensure that the leadership team and relevant staff are:

- aware of and understand the systems in place
- manage them effectively
- know how to escalate concerns when identified.

Schools and colleges should use communications with parents and carers to reinforce the importance of children being safe online. Schools should share information with parents/carers about:
what systems they have in place to filter and monitor online use

- what they are asking children to do online, including the sites they will asked to access
- who from the school or college (if anyone) their child is going to be interacting with online.

14. Monitoring arrangements

All connections to the internet are monitored, and where possible capturing the username, date, time and URL that is accessed. All academies use Senso to monitor ~~internet usage~~ computer use, on compatible devices. DSL and safeguarding teams will be informed of any concerns.

Commented [SWCC1]: Section 14. Slight amendment below to be clear that all internet is monitored everywhere, and on compatible devices Senso is used to provide device based monitoring (screen/keyboard capture).

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 IT 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.

15. Links with other policies and guidance

This online safety policy is linked to our:

- Remote Education guidance
- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Acceptable Use agreement – Please note this statement is for all users and will require guidance and further support to read and access for younger pupils or students with additional needs.

CLF IT Acceptable Use Agreement

This agreement sets out the requirements with which you must comply when using the CLF's IT equipment.

Property: You should treat any property belonging to the CLF with respect and reasonable care and report any faults or breakages immediately to the IT team.

Leaving workstations: If you leave your workstation for **any** period of time you should take appropriate action by either logging off or locking your computer by pressing the Windows key and "L". **You** are responsible for keeping your login secure.

Monitoring: The CLF uses software which automatically monitors computer usage.
The monitoring is carried out by a number of systems, if anything of concern is revealed as a result of such monitoring then this information may be shared with those investigating the concern. In exceptional circumstances concerns will need to be referred to external agencies such as the Police.

Unsuitable material: Viewing or Downloading of inappropriate material, at any time, is strictly prohibited. Internet access may be withdrawn without notice at the discretion of the Principal or appropriate senior manager whilst allegations of unsuitable use are investigated.

Emails: Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to our equal opportunities policy), or defamatory is not permitted. In doing so you may have your Email account disabled.

Viruses and other malicious code: You should be aware of the potential damage that can be caused by computer viruses and other malicious code. You must not introduce or operate any hardware/software or open suspicious links in emails which have not first been checked by the CLF IT Team's for viruses.

***For Staff Only please refer to the CLF Employment Manual for further details.**