Four Cs
Multi-Academy Trust

Curiosity Confidence Courage Constancy

E-Safety Policy

Presented to
Trustees Standards Committee
3 October 2024

Date approved:[1]	3 October 2024
Date reviewed:[2]	
Date of next review:[3]	Autumn 2027

[1] This is the date the policy was approved by the meeting
[2] This is the date the policy was reviewed prior to its approval above
[3] This is the date as set by the policy review clause or the date approved plus three years

1. Purpose and aims of the policy

Digital and online technologies have become an integral part of the Trust's operations. Clear rules, procedures, and guidelines must be established to minimise risks.

1.1 The most common areas of risk to students are:

- Contact: Subject to harmful online interactions with other users; being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Content: Exposure to illegal, inappropriate, or harmful material; being exposed to illegal, inappropriate, or harmful content, for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- Conduct: The individual's online risky behaviour that then leads to harm; online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (eg consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- Commerce: Online commerce (online gambling, inappropriate advertising, phishing, or financial scams); commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

1.2 All staff must be clear about appropriate procedures to protect the Trust, all its members and themselves.

1.3 The Trust acknowledges that whilst it endeavours to safeguard against all risks, it may never be able to eliminate them all due to the evolving nature of online threats. Any incidents that may arise will be dealt with quickly and according to policy to ensure that all members of the Trust community are protected. The Trust will endeavour to develop and improve systems and protections as it becomes aware of new threats and risks.

1.4 The policy aims to:

- Ensure the safeguarding of all students/pupils within and beyond academy settings.
- Protect all Trust staff within and beyond Trust settings.
- Protect the Trust from any negative impacts caused by harm or threat to any of its uses of digital technologies, whether these be of accidental or malicious cause.
- Provide clarity about Trust procedures and the roles and responsibilities of all involved.

2. General Data Protection Principles

This policy must be read in conjunction with the Four Cs Trust General Data Protection Regulations Policy and the Trust's Staff ICT Policy. The Four Cs Trust will refer to the most recent government, Department for Education (DfE), and Information Commissioners Office (ICO) guidance and documentation regarding data protection, data storage, and privacy compliance. Personal data will be recorded, processed, transferred, and made available according to the Trust Data Protection Policy and in compliance with GDPR and the Data Protection Act (1998).

3. Scope of the policy

3.1 This policy applies to all members of the Four Cs Trust community (including staff, students/pupils, volunteers, parents/carers, Trustees/Governors, visitors, and community users) who have been given access to and use ICT systems both in and out of Four Cs Trust academy sites.

3.2 The Four Cs Trust expects all academies to make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding the use of technology and the Internet both on and off the academy sites. This will include imposing sanctions for behaviour - as defined under the Education and Inspections Act 2006. The 'In Loco Parentis' duty allows the Trust/academies to report and act on instances of cyberbullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material, including reporting to the police, social media websites, and hosting providers on behalf of students/pupils.

3.3 The academies will deal with such incidents within this policy and associated behaviour and anti-bullying policies. Where known, they will inform parents/carers of incidents of inappropriate E-safety behaviour that take place outside of academy sites.

3.4 The policy also covers the contents and use of personal electronic equipment on academy sites.

3.5 As identified by Keeping Children Safe in Education, this policy recognises that technology plays a significant role in children's lives, and abuse can take place concurrently online and in daily life. Therefore, Online safety must be considered part of a whole Trust approach.
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

3.6 The E-safety policy covers the use of:

- Academy-based IT systems and cloud-based software.
- Academy-based intranet and networking.
- Academy-related external Internet, including but not exclusively e-learning platforms, blogs, and social media websites.
- External access to internal academy cloud platforms, eg Google Drive, Microsoft 365.
- Academy IT equipment off-site, for example, staff laptops, digital cameras, mobile phones, tablets, dongles and similar.
- Student and staff personal IT equipment when used in the academy and which makes use of the academy networking, file-sharing, or Internet facilities.
- Tablets, mobile phones, devices, and laptops when used on the academy sites.

4. Roles and responsibilities

4.1 Principal/Headteacher and Senior Leadership Team

It is the overall responsibility of the Principal/Headteacher and Senior Leadership Team to ensure that E-safety and Digital Security (referring to keeping IT systems secure) are well-managed in each academy:

- The Principal/Headteacher and Senior Leadership Team are responsible for promoting E-safety and Digital Security throughout their respective academy.
- They will implement agreed policies, procedures and staff training, taking the lead responsibility for ensuring E-Safety and Digital Security are addressed to establish a safe learning and working environment.
- The Principal/Headteacher will inform Governors/Trustees about the delivery of the E-safety curriculum, ensuring they understand how this relates to child protection.
- The Principal/Headteacher will inform the Governors/Trustees about promoting and maintaining Digital Security.
- The Principal/Headteacher and Senior Leadership Team are responsible for determining, evaluating and reviewing online safety to encompass teaching and learning, use of academy IT equipment and facilities by students/pupils, staff and visitors, and agreed criteria for acceptable use by students/pupils, academy staff and Trustees of Internet-capable equipment for academy related purposes, or in situations which will impact on the reputation of the academy, and/or on academy

premises. This is in line with expectations in Keeping Children Safe in Education in relation to an annual review/risk assessment of online safety provision.

- The Principal/Headteacher and Senior Leadership Team are responsible for the regular assessment of the strengths and weaknesses of practice within their respective academy to help determine the training provision needed for staff and guidance provided to all staff, students/pupils, volunteers, parents/carers, Trustees, Governors, visitors, and community users.

4.2 Academy E-safety Leads / DSL responsible

It is the role of each academy's designated E-safety lead to:

- Responsible for online safety issues on a day-to-day basis, liaising with relevant stakeholders, including IT support, the Trust's Safeguarding Leader, and other Trust contacts, to ensure the safety of students/pupils.
- Liaise with the PSHE/Citizenship and Ethics, DSLs, and Computing/ICT leads to ensure that all policies and procedures are up to date and take account of any emerging issues and technologies.
- Provide up-to-date information for all staff to teach and manage E-safety effectively.
- Involve parents/carers so they feel informed and know where to seek advice.
- Develop and maintain staff awareness of the nature and likelihood of phishing and cyber-attacks. Train staff to be alert to the typical signs of such attacks and to know how to best protect themselves, the academies, and the wider Trust from them.
- Have an overview of all academy digital/online technology usage—it is a teacher's responsibility to monitor the students/pupils in their care's usage.
- Keep a log of incidents for analysis to help inform future development and safeguarding.
- Report issues to the Trust IT Services and regularly update the Principal/Headteacher.
- Be involved in any risk assessment of new technologies, services, or software to analyse potential risks.
- Attend relevant meetings of Governors/Trustees/SLT meetings when requested.
- Where required, be responsible for escalating online safety incidents to the relevant external parties, eg CEOP, Cyber Choices, National Cyber Security Centre, local Police, Local Safeguarding Children's Board, social care, etc.

4.3 Trust IT Services

Trust IT Services staff are responsible for:

- Securing the network and infrastructure of the academies, reviewing activity regularly.
- Ensuring that users comply with basic access policies and that only trusted devices can connect to the academy network.
- Filtering of search facilities is robust and regularly checked for penetration to ensure that the risk of students/pupils accessing unsuitable material is minimised.
- To keep up to date with current threats and attack trends and take steps to mitigate this and communicate with each academy's leadership team and E-safety lead.
- Reporting to each academy's leadership team and E-safety lead on any network intrusions or other threats to the network.
- Ensuring that any IT outsourced, eg connectivity, maintenance, cloud-based services website, email provision, filtering, anti-virus, complies with DfE guidance and Data Protection regulations.
- Promoting basic cyber security practices within the academies, eg locking computers when away from the desk, using secure passwords, and caution when using USB removable drives.
- Ensuring there is appropriate and up-to-date anti-virus and anti-spyware software on all susceptible devices and that this is reviewed and updated regularly.
- Ensuring that filtering is set to the correct level for staff and students/pupils at the initial set-up of all devices and within any online environments.

- Ensuring that all users may only access the academy's networks through a properly enforced password protection policy that requires regular password changes.

4.4 All Staff/Adults in an Academy

It is the responsibility of all staff/adults within each academy to:

- Ensure that they know who the Designated Person for Child Protection is so that incidents involving students/pupils can be reported. Where an allegation is made against a member of staff, it should be reported immediately to the Principal/Headteacher. In the event of an allegation made against the Principal, the CEO/Chair of Governors must be informed immediately.
- Ensure they have read and understood the academy's/Trust's Staff ICT Policies.
- Report incidents of cyber-bullying or other inappropriate behaviour via digital technologies in line with each academy's incident reporting process.
- Be up to date with E-safety knowledge appropriate for the age group they work with and embed this throughout the curriculum regardless of role.
- Ensure that all students/pupils are protected and supported in their use of online technologies so that they know how to use them safely and responsibly and know what to do in the event of an incident.
- Monitor students/pupils' choices of passwords within any online environment.
- Respond promptly if a student/pupil believes others know any of their passwords.
- Only upload student/pupil information, as required by specific job roles, to online databases requiring services (for example, MIS or assessment system) for agreed purposes*, such as monitoring pupil progress and/or enhancing their learning. *Such service providers must have been approved by the school and approved by the Trust Data Protection Officer (DPO).
- Alert the E-safety lead of any new or arising issues and risks that may need to be included within policies and procedures.
- As part of the overall staff induction procedures, all staff will receive an online safety induction and attend mandatory online safety training provided by the academy or the Safeguarding Lead.
- Be vigilant in monitoring student/pupil Internet and computer usage to ensure compliance with the policy. This may include using personal technology, such as cameras and phones, on the academy site where there is a cause for concern.
- Internet usage and suggested websites should be pre-vetted and documented in lesson planning.
- Staff must promote and reinforce safe online practices on and off-site, including advising students/pupils on reporting incidents.

4.5 All Staff/Adults in the Trust

In addition to the responsibilities of staff/adults in each academy, it is the responsibility of all staff/adults within the Trust (this includes those staff/adults who are not based at an academy site) to:

- Be aware of the Prevent (Radicalisation) Agenda and act appropriately upon any concerns.
- Keep academy/Trust information confidential and do not breach the Data Protection Act.
- Not disclose security passwords or leave a device unattended when logged in.
- Follow security procedures if any data is required to be taken from the Trust premises.
- Use caution and measures such as installed anti-virus software to prevent the transfer of viruses to a Trust network from removable media and the internet.
- Be alert to the signs of phishing/cyber-attacks, eg anything unexpected about the arrival, nature or layout of an email, especially if it invites the recipient to click on a button, follow a link or open an attachment. Such emails should be deleted, or further enquiries made.
- Report any accidental 'misuse' or access to inappropriate materials to a senior line manager.

- Appropriately use only devices provided by (or authorised by) an academy/the Trust. Any use of personal equipment required should be agreed upon or reported promptly to a senior line manager.
- Only use academy/Trust-provided USB memory sticks and follow agreed encryption procedures.
- Use devices provided by the academy/Trust when working at home/remotely or ensure that any personal devices used for work purposes at home have up-to-date anti-virus and malware protection and are password protected.

4.6 Academy Pupils

Students/Pupils will be:

- Taught to use digital/online technologies safely and responsibly through Computing/ICT, PSHE and across the curriculum in both primary and secondary phases.
- Taught to tell a trusted adult about any concerns relating to their use of digital technologies or any other issues causing distress straightaway. Students/pupils are responsible for ensuring they report online safety incidents in the academy or with other external reporting facilities, such as CEOP or Childline, and are expected:
    - To be aware of and comply with academy policies for Internet and mobile technology usage in the academy, including the use of personal items such as mobile phones.
    - To be aware that their internet use out of the academy on social networking sites is covered under the Online Safety Policy if it impacts on the academy and/or its staff and students in terms of cyber bullying, reputation, or illegal activities.
    - To follow basic cyber security practices within the academy eg locking computers when away from the desk, using secure passwords, and caution with the use of USB drives.
- As students/pupils get older they will increasingly:
    - Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
    - Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- Students are expected to have a good understanding of research skills, the need to avoid plagiarism, and the need to uphold copyright regulations.
- In primary phases students/pupils should not be in possession of any wearable technology, for example, smart watches, that has cellular capability (the ability to communicate with other devices inside or outside of school)

4.7 Academy Parents/Carers

The Trust wants parents/carers to feel involved and active in their children's E-safety education. Each academy will keep parents informed about potential risks and current best guidance.

- Parents should know where to go for advice and support, starting with their child's class teacher in the primary phases and the student/pupil's tutor in the secondary phases. This support should be clear that it extends beyond the school day and gates; it is more likely that issues will occur outside of schools rather than within.
- Parents/carers must support the academy in promoting good Internet behaviour and responsible use of IT equipment and mobile technologies both at the academy and at home.
- Parents can communicate with the relevant academy via their academy's communication policy, following clear protocols and rules. All such communications must be polite and related to school matters only.

4.8 Governors/Trustees

Governors and Trustees will:

- Ensure Child Protection is covered with an awareness of E-safety and be clear on how it is addressed within each academy. The Governors/Trustees are responsible for ensuring that all Child Protection guidance and practices are embedded.
- In collaboration with the Principal/Headteacher jointly ensure that any misuse or incident is dealt with according to policy and appropriate action is taken to extremes such as suspending a member of staff, excluding a student/pupil or involving the Police.

5. Remote Education

Academies will follow the DfE's 'Providing remote education: guidance for schools' after the expiration of the temporary arrangements in the Coronavirus Act 2020 in relation to remote education.
https://www.gov.uk/government/publications/providing-remote-education-guidance-for-schools/providing-remote-education-guidance-for-schools
Providing remote education: guidance for schools - GOV.UK

6. Standards and Expectations

6.1 Systems

- Academy computer systems will be configured to meet the academy's teaching and learning requirements while maintaining online safety.
- Risk management exercises completed when a system change or a new software package is purchased, for example.
- Systems will be compliant with the academy, Trust, local authority, DfE, ICO and Data Protection guidelines about online safety procedures being met.
- Regular audits and evaluations of the network will be carried out, identifying areas for improvement. These improvements will be raised with The Four Cs Trust Leadership team.
- Academy IT staff will be responsible for monitoring IT use.

6.2 Filtering and Monitoring

- The Trust uses an accredited filtering system, Classroom.Cloud. Filtering reports and logs from this system will be examined regularly.
- Any filtering incidents are examined, and action taken and recorded to prevent a recurrence. The Trust will provide enhanced/differentiated user-level filtering.
- Internet access will be filtered for all users.
- If the IT Manager (or another person) needs to switch off the filtering for any reason or for any user, the Principal/Headteacher must record and agree to this.
- Any filtering issues should be reported immediately to IT staff.
- Staff requests for websites to be removed from the filtered list will be considered by the IT Manager and confirmed with the Principal/Headteacher or delegated Senior Leader in the respective academy if necessary.

6.3 Network Security

- All users will have clearly defined access rights to academy technical systems and devices.
- Trust IT staff will provide all users with a username and secure password. Users are responsible for the security of their username and password in accordance with the current password requirements outlined by the IT Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, etc from accidental or malicious attempts that might threaten the security of the academy systems and data.
- Servers, wireless systems and cabling must be securely located and physical access restricted.

- Appropriate security measures are in place to protect the servers, routers, switches, wireless systems and workstations from accidental or malicious attempts which might threaten the security of the Trust systems and data.
- Staff are forbidden from installing programs on Trust devices without the prior consent of the IT Manager.
- The Trust's infrastructure and individual workstations are protected by up-to-date virus software.

6.4 Use of images and videos

- Each academy will ensure images and videos of students, staff, student/pupils' work and any other personally identifying material are used, stored, archived, and published in line with the Data Protection Act, ICO guidance for schools, DfE guidance for schools and the Acceptable Use Policy.
- Academy images of students/pupils will not be compromising or inappropriate. If a member of staff is unsure if a photograph is appropriate for publication, they should seek guidance from the Senior Leadership Team.
- Images/videos of students/pupils can only be taken on academy devices and stored securely on the school network; they can never be taken on personal devices such as mobile phones.
- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images, in particular the risks attached to publishing their own images on the internet such as on social media.
- Written permission from parents/carers will be obtained before photographs of students/pupils are published on the academy website, social media, or local press.
- In accordance with the ICO's guidance, parents/carers are able to take videos and digital images of their children at academy events for their own personal use but should not make them publicly available if other students/pupils are involved in the digital image or video.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission.
- Students/pupils full names will not be used anywhere on a website, social media, or home-school contact platform, eg Class Dojo, particularly in association with photographs.

7. Appropriate Use

7.1 Appropriate Use by Trust staff/adults

Staff members with password-protected access to the Trust/academy networks have this to access, develop and manage appropriate resources for their work within the Trust and individual academies. Staff also have access to a range of peripheral ICT, for example, visualisers, scanning equipment etc, that is similarly resourced/supplied to appropriately deliver the work of the Trust/its academies.

7.2 In the event of Inappropriate Use by Trust Staff/Adults

If a Trust employee is believed to have deliberately misused any of the Trust's digital/online resources in any manner felt to be inappropriate, a report must be made to the staff member's Principal/Headteacher or Senior Manager immediately and this will be dealt with in line with Code of Conduct for All Adults policy.

7.3 Appropriate Use by Academy Students/Pupils

Within the Trust students/pupils are taught to use digital/online technologies safely and responsibly, for example, knowing how to conduct research or write a message to another pupil. The downloading of content should be 'fit for purpose' eg based on research for work. Students/pupils will be taught about the implications of misusing digital/online technologies eg posting hurtful/inappropriate material online. If a student/pupil accidentally accesses upsetting or inappropriate content the student/pupil

should know appropriate actions to take, for example, close the page and report this to a staff member immediately. Where a student/pupil feels unable to disclose any issues or misuses against them to a trusted adult, they should have been made aware of the facilities such as the CEOP Report Abuse button (www.thinkuknow.co.uk) and Childline number (0800 1111) to seek advice and help.

7.4 In the event of Inappropriate Use by Academy Students/Pupils – Internal/inside of school

Should a student/pupil be found to have deliberately misused digital/online resources the academy where the child attends will follow their behaviour policy, but the following consequences will occur:

- The parents/carers of the student/pupil will be contacted.
- A formal incident record will be made.
- Further or serious misuse of the rules may result in a suspension of access to some digital/online resources.
- Depending on the seriousness of the incident other sanctions may be employed. This will be overseen by the Principal/Headteacher in line with support from Governors/Trustees.

7.5 In the event of Inappropriate Use by Academy Students/Pupils – External/outside of school

If the academy becomes aware of an incident outside of school, it will raise this with any parents/carers involved and offer guidance toward its resolution. In extreme cases, some such situations may require the contacting of outside agencies such as the police, or an appropriate body. In cases of 'youth produced sexual imagery', (a specific definition of 'sexting') an academy will follow 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'.

8. Curriculum

8.1 All students/pupils will be taught to use online technologies safely and responsibly

They must use the Internet safely to research information, explore concepts, deepen knowledge, and communicate effectively to further learning. This will be done through ICT/computing and PSHE/Citizenship and Ethics lessons and across the wider curriculum areas.

The following concepts, skills and understanding will be taught in all academies:

- Internet literacy, including making good judgements about websites.
- understanding risks such as viruses and opening mail from a stranger.
- knowledge of copyright, plagiarism, file-sharing and downloading illegal content issues.
- data privacy awareness – knowing what is and is not safe to upload.
- how to access appropriate guidance, where to go for advice and how to report abuse.

All academies within the Trust use the DfE non-statutory guidance 'Teaching online safety in schools, 2023' to support the teaching of E-safety.
https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

8.2 Internet Usage

- In lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material found in internet searches.
- Where students/pupils are allowed to freely search the Internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that on occasion, for educational reasons, students/pupils may need to research topics (eg racism, drugs, and discrimination) that would normally result in blocked internet searches. This is done in a controlled environment under the supervision of the classroom teacher.

9. Communications

9.1 Academy/Trust staff can communicate with students/pupils' parents via their academy/Trust email address, following clear protocols and rules set by each academy.

- All such communications must be:
  - Professional and related to school matters only.
  - Reflect a suitable tone/content and ensure that the reputation of the academy and Trust is maintained.
  - Only sent when a school is open to students/pupils.
- There are cloud systems in place for storing all electronic communications, eg emails, between academies, parents/carers and students/pupils. These can be monitored and checked as needed.
- Primary-age students/pupils must never be contacted directly by any means other than by academy-set-up/approved systems such as Seesaw/Class Dojo/Tapestry and only when the academy allows staff to do so.
- Secondary-age pupils may be appropriately (as above) communicated with via their school-provided email addresses. Under no circumstances will staff contact students/pupils or parents/carers or conduct any school business using a personal email address.
- Staff should not use personal phones in classrooms or other areas of the school where they are with students/pupils. Unless directed to do so by a senior staff member, staff should not use their personal phones to contact parents/carers. Where this has been permitted, for example, staff must hide their caller ID at the end of a school trip. Staff must never contact students/pupils using their personal phones.
- Users must immediately report to the nominated person (eg class teacher, E-safety lead) the receipt of any email that makes them feel uncomfortable or is offensive, threatening, or bullying in nature. They must not respond.

9.2 <u>Academy Students/Pupils' Mobile Phones and other Electronic Devices or Accessories</u>

<u>Primary phase students/pupils</u>:
Without the express permission of a Principal/Headteacher or designated senior leader, children are not allowed to use mobile phones on school grounds during the school day, at after-school clubs, on a school trip, or on residential visits. It is recognised that some students/pupils may need a mobile phone, for example, if they are travelling on public transport to be in school. In these cases, the mobile phone should be left in the main school office for the day.

<u>Secondary phase students/pupils</u>:
Mobile phones and any other electronic devices or accessories must not be used, seen, or heard during the school day. In the event of inappropriate use, sanctions, such as removing a student's/pupils' right to have a device on the school premises, will be taken in line with each academy's mobile phone / behaviour policy.

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Publishing such material on a website which causes distress to someone will be considered a breach of the academy's behaviour policy, intentional or unintentional. The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress is online bullying, which will be dealt with in line with the academy's behaviour policy.

10. Monitoring and Review

The Trustee Standards Committee has the responsibility for implementing, monitoring and reviewing this policy. Any issues, which arise, which do not fall within the remit of this Committee or are relevant to other areas of the Trust, will be brought to the attention of the relevant committees and /or individuals.

The Trustees will review this policy in line with the procedure for policy review.

Date for review - if no other reason for review (see policy review procedure) this policy will be reviewed every three years.