



CONNECT
MULTI-ACADEMY TRUST

Acceptable Use and Online Safety Policy

Policy Owner	Kevin Broadfoot
---------------------	------------------------

Review date	Version No.	Approved by	Date approved	Effective from
May 2024	3.0	ATB	May 2021	May 2021
Sept 2025	4.0	Resources Committee	Sept 2025	Sept 2025
Sept 2026	5.0	Standards Committee	Sept 2026	Sept 2026

Student Acceptable Use Policy



Item	Contents	Page
1	Introduction	3
2	Purpose & Definitions	3
3	Trust Responsibilities	4
4	Safeguarding and Online Safety	4
5	Student Responsibilities	5
6	Mobile Phones	6
7	Social Networking	8
8	Cyber Bullying	9
9	Monitoring and Review	



Student Acceptable Use and Online Safety Policy

1. Introduction

Connect Multi Academy Trust provide computer equipment and network at its Academies with internet and email access for students. This access supports to a vast amount of information for use in studies but there are dangers and this policy details rules for the safe and legal use of the ICT resources in our Academies. The computer network is provided for the benefit of all students, and students are encouraged to use and enjoy these resources, and to help to ensure they remain available to all.

Students are responsible for good behaviour both when using the ICT resources and when using online resources and tools just as they are in other aspects of Academy life. It is important to remember that access to the computer network, online resources, the internet and email is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

2. Purpose & Definitions

This policy ensures that all children use digital technologies responsibly, safely, and ethically. It applies to all IT systems, devices, online resources, internet services, artificial intelligence and digital tools provided or accessed within our secondary schools. A definition of terms is found in Appendix 2.

This policy strengthens safeguarding by reducing risks associated with cyberbullying, inappropriate recording, harmful content, and disruption to learning. Any misuse involving bullying, harmful images, social media abuse, or other safeguarding concerns will be addressed in line with behaviour and safeguarding procedures.

This policy will identify approaches to educate and raise awareness of online safety within the community and identify clear procedures to use when responding to online safety concerns.

This policy applies to:

- All students enrolled within Connect Multi Academy Trust schools.
- All devices and systems provided by the Trust or used on Trust premises.
- All online activity conducted during / after school hours related to school or on school devices.

This policy takes into account the DfE statutory guidance [Keeping children safe in education 2026](#), [EYFS statutory framework for group and school-based providers 2026](#), 'Working Together to Safeguard Children 2026' and the Digital and Technology Standards.

This should be read in conjunction with the following policies:

- o Anti-bullying policy
- o Behaviour for Learning Policy
- o Safeguarding and Child Protection Policy
- o Cyber Security Plan
- o Data Protection Policy



3. Trust Responsibilities

The Trust is responsible for ensuring that the system in which the students access digital and online resources is safe, secure and ensures compliance to [Keeping children safe in education 2026](#), [EYFS statutory framework for group and school-based providers 2026](#), [Working Together to Safeguard Children 2026](#) and the Digital and Technology Standards.

The Trust will ensure that all its schools are provided with an up to date, filtered and monitored network and internet connection using Smoothwall Filters and Firewalls and Smoothwall Monitor as outlined in section 4. The filter and monitoring system is reviewed annually in line with DfE digital and technology standards.

The Trust along with its schools are responsible for developing the use of technologies and developing a curriculum to support students' knowledge, learning and wellbeing by adopting this policy and for ensuring that students are safe.

The use of Trust equipment will be considered as deemed as the student's acceptance of this policy.

4. Safeguarding and Online Safety

The schools within the Trust provide a filtered and monitored network and internet connectivity using Smoothwall Filters and Firewalls and Smoothwall monitor to keep students safe from inappropriate online material, from internal communication and protect Academy systems. The system will identify searches, websites, online activity, communications or other activity that are deemed inappropriate or that may indicate a safeguarding or security concern.

Alerts will be reviewed by authorised staff and, where appropriate, referred to the Designated Safeguarding Lead or other relevant staff. In serious incidents the Designated Safeguarding Lead will be contacted by the software to ensure that support is delivered immediately.

Filtering and monitoring systems cannot prevent or identify every risk. Students must report anything that makes them feel unsafe or uncomfortable, even if the website or content has not been blocked.

The Filters and Monitoring software are kept up to date with the latest information coming from DfE, Police and other agencies but will ensure that the students are protected from the following:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact:** being subjected to harmful online interaction with other users including blocking all social media platforms.
- **Conduct:** the internal filter will monitor and flag inappropriate peer to peer contact and report this to the appropriate member of staff and personal online or digital behaviour that increases the likelihood of, or causes, harm
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.



5. Student Responsibilities

Students are responsible for looking after the IT and digital resources and using them in an acceptable manner, ensuring that IT and digital resources are used for educational purposes and that staff instructions are followed when using devices. The following outlines the acceptable use of the IT and digital resources by students. This is not an exhaustive list; other incidences may be deemed to be a breach of this policy.

5.1 Equipment

- Damaging, disabling or otherwise impairing the operation of computers and other ICT equipment will be considered as an act of vandalism;
- Academy devices, online digital resources, internet and email system are for educational use only;
- Files brought in on removable media such as USB flash drives will be virus-checked before copying them onto the network;
- The use of personal equipment such as laptops, tablets, mobile phones or other computer devices capable of internet access and/or electronic data storage in the Academy is strictly forbidden without Head Teacher permission and a signed parental permission form and acceptance that the device will be filtered and monitored using our safeguarding tools;
- Personal computing equipment that has been authorised for use in the Academy will be connected to a guest network and online activity will be filtered and monitored;
- Eating and drinking near any computer equipment is strictly forbidden. This is necessary to protect the computers from accidental spillages which could cause serious damage and create the danger of electric shock.

5.2 Network

Students are given their own username and password to access the school network.

- Sharing of passwords with anyone else is strictly forbidden;
- Students should never use any other user's login details. Logging in using someone else's username and password is not permitted;
- The storing of pornographic, homophobic, racist or other material deemed offensive on the network is strictly forbidden and will be monitored using the safeguarding software;
- Playing games on Academy devices is not permitted;
- Students are responsible for the security of their own user area, and will be held fully accountable for any abuse of, or originating from their account.

5.3 Security

Students should always respect the security on the school's computer network

- Activity that threatens the integrity of the IT and digital systems, or activity that attacks or corrupts other systems is strictly forbidden
- Deliberate meddling with viruses and hacking is a serious criminal offence and will result in contacting the police and sanctions outlined in the Behaviour for Learning Policy.
- Students must never reveal their personal details, including full name, home address, telephone number or provide an image, video or avatar of themselves.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted in any way



- Student user storage areas, files, Internet and email usage will be checked regularly to ensure that they are using the Academy ICT facilities responsibly

5.4 Internet and Online Safety

The schools have a filtered and monitored network and internet connectivity, students have a responsibility to work within the system to ensure their safety. Filtering and monitoring systems cannot prevent or identify every risk.

- Students must report anything that makes them feel unsafe or uncomfortable, even if the website or content has not been blocked.
- Schools will provide a monitoring system that will highlight and capture any activity it deems is not within the policy settings.
- Any attempt to bypass the school's internet filtering or monitoring system will result in sanctions outlined in the Behaviour Policy.
- Internet access in the schools is for educational use only
- Use of the internet to access, download, send, print display or otherwise transmit in appropriate, pornographic, racist, violent, offensive or any illegal material is strictly forbidden.
- Students must not share sexual images or videos, of themselves("Nudes") or others, participate in any sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media.
- Students must report if they find any terrorist or extremist material when accessing the internet on site.
- Students must not share online hate content, directed towards or posted by specific members of the school or community
- Students are not permitted to download games on school computers
- Use for financial gain, gambling, political purposes or advertising is not permitted
- The use of social media, chat rooms and instant messaging is forbidden unless specifically authorised by a teacher for educational use as part of a planned lesson
- Copyright laws must be respected at all times. Respect the work and ownership rights of people outside the Trust, as well as other students or staff
- The download or storage of media files of any kind is not permitted unless specifically authorised by a teacher

5.5 Use of Artificial Intelligence (AI)

AI tools (e.g., chatbots, image generators, coding assistants) are blocked by default but may be used under supervision for educational purposes. Students must:

- Use AI ethically and responsibly.
- Avoid using AI to plagiarise or cheat.
- Clearly label AI-generated content when submitting work.
- Never use AI to impersonate others or create misleading content.
- Not generate inappropriate, discriminatory, harmful, or offensive material.
- Not enter personal, confidential or sensitive information into an AI system
- Not create or sharing deceptive content, including Deep Fakes. Deep Fakes are digitally altered videos, images, or audio that falsely represent someone's actions or words.

6. Mobile Phones and Smart Technology

This policy adheres to the "mobile phones in schools" guidance which became statutory on 29 June 2026, with schools following it from 1 September 2026.



The key points are:

- Schools should be mobile-phone-free by default. The DfE expects schools to prohibit pupils' access to mobile phones throughout the whole school day. This includes lessons, movement between lessons, breaktimes and lunchtime.
- This policy also covers similar smart devices capable of sending/receiving messages or notifications or recording audio/video.

The Trust is committed to ensuring that learning is paramount; expectations are high and safeguarding standards remain robust. Therefore, mobile phones, smartwatches and other wearable technology capable of sending or receiving messages, accessing the internet, recording audio/video or displaying notifications must not be worn or used during the school days.

This policy establishes clear expectations regarding the use of mobile phones and smart technology in order to maintain a calm, safe and disruption-free learning environment.

The policy is underpinned by statutory powers contained within the Education and Inspections Act 2006, the Education Act 2011 and current DfE Searching, Screening and Confiscation guidance.

Students and their parents/carers must understand this policy before students are given permission to bring mobile phones into schools.

Children may bring a mobile phone to school; however, it must remain switched off and out of sight for the entire school day. Devices must not be seen, heard or used during lessons, transitions, break times or lunchtime.

This policy also applies to students during external visits and extra-curricular activities. This policy applies to all pupils whilst on school premises or otherwise under the lawful control of the school, including educational visits and residential trips.

Breaches of this policy will be addressed in line with the School's Behaviour for Learning (BfL) escalation system. However, the escalation process is outlined below:

First Offence:

- Confiscation – the device will be stored securely in Student Reception.
- Student will be issued with an after-school detention.
- School will contact the parent or carer to collect the phone from reception.
- Letter to parents
- The school may undertake proportionate checks to establish compliance with the mobile-phone policy.

Second Offence:

- Confiscation – the device will be stored securely at Pupil Reception.
- Pupil will receive one day in the learning support unit
- School will contact the Parent or Carer to collect the phone.
- Ban from bringing a mobile device onto school premises for 6 months.
- Letter to parent
- The school may undertake proportionate checks to establish compliance with the mobile-phone policy.



Third Offence:

- Using a phone whilst on a ban or a 3rd offence.
- Confiscation – the device will be stored securely in pupil reception
- Pupil will receive a suspension (C6)
- Call to parent or carer to collect the phone
- Life ban from bringing a mobile device onto school premises.
- Letter to parent
- The school may undertake proportionate checks to establish compliance with the mobile-phone policy.

Failure to comply with staff will result in sanctions in accordance with the Behaviour for Learning Policy.

Staff have the statutory power to confiscate a mobile phone where it is used in breach of this policy. Under Section 91 of the Education and Inspections Act 2006, staff may confiscate, retain or dispose of a pupil's property as a disciplinary penalty where reasonable.

Staff are protected from liability for loss or damage to confiscated items provided they have acted lawfully.

Designated staff may search pupils where there are reasonable grounds to suspect possession of banned or prohibited items, including suspicion of inappropriate mobile phone use. Searches will be conducted in accordance with statutory guidance. Any search of a pupil or their possessions will be conducted in accordance with the school's Searching, Screening and Confiscation procedures and applicable statutory guidance

Where there is a 'good reason', authorised staff may examine data or files on an electronic device and may erase data where appropriate. In cases involving safeguarding concerns, the Designated Safeguarding Lead (DSL) will determine whether material should be deleted, retained as evidence, or referred to the police.

The schools accept no responsibility for replacing lost, stolen or damaged mobile phones. The school accepts no responsibility for students who lose or have their mobile phones stolen while travelling to and from the Academy

Our schools will operate their own system to ensure the site remains a mobile phone-free environment. One such system is the Yondr pouch system. If the school operates this system, then the students should comply with the following:

- All students are required to place their switched-off mobile phone into a Yondr pouch upon arrival.
- The pouch remains locked for the duration of the school day and will be unlocked at designated exit points.
- Pupils must keep the pouch with them at all times.
- Failure to place a device into a pouch, tampering with or damaging a pouch, or attempting to bypass the system will be treated as a serious breach and escalated through the Behaviour for Learning system..
- Students that have forgotten the pouch should hand in their phone immediately, without being asked.
- Repeat offenders will result in further sanctions.
- Parents are responsible for replacing lost pouches. Until a replacement is provided, the students will should follow the 'forgotten pouch' procedure.

The Trust recognises its duties under the Equality Act 2010. Reasonable adjustments may be agreed in advance for students with medical or additional needs. Any exception will be formally documented and limited to a defined purpose, time and location.



In an emergency, pupils should follow the instructions of staff. The school will make appropriate arrangements for communication with parents/carers and emergency services. Pupils must not independently use mobile phones unless instructed or an agreed exception applies.

7. Social Media Sites

By default, Social Media Sites are blocked by the filter. Social networking applications include, online discussion forums; collaborative spaces, such as Facebook, Instagram and SnapChat; media sharing services, for example YouTube, Twitter and others.

The widespread availability and use of social networking application brings opportunities to understand, engage and communicate with audiences in new ways. However, it is important to protect the school's reputation and ensure students are safeguarded.

- No student may access social networking sites during the academy day or whilst on the school premises
- No computers are to be used to access social networking sites at any time of day
- Any attempts to breach firewalls will result in a ban from using academy ICT equipment other than with close supervision
- Where a disclosure of social networking bullying is made which originates outside of the school, then the school will investigate on occasions where the bullying impacts on the student in school. It is the responsibility of parents to monitor social networking access by their child outside of the academy day. Parents should be aware of the age restrictions for accessing social networking sites.

8. Cyber-Bullying

The Trust's anti-bullying position is the belief that 'all students have a right not to be bullied' and that 'bullying is always unacceptable'. The Trust also recognises that it must 'take note of bullying perpetrated outside the School which spills over into the School'. Under powers granted by the EIA 2006, the Head Teacher is able to police cyber-bullying or any bullying aspects carried out by students even at home.

Definition of Cyber Bullying

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend themselves.

By cyber-bullying, we mean bullying by electronic media:

- Bullying by texts or direct/group messages or calls on mobile phones or other platforms.
- The use of video or AI to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, group chats, personal websites or social networking sites
- Using e-mail to message others
- Creating or sharing sexual images or videos, of themselves("Nudes") or others to participate in any sexualised online coercion and threats or unwanted sexual comments.



- Hijacking/cloning e-mail / social media accounts
- Making threatening, abusive, defamatory or humiliating remarks on social media

School Responsibility

Connect Multi Academies Trust educates its students both in the proper use of communication and about the serious consequences of cyber-bullying and will, through PHSE and in IT lessons and assemblies, continue to inform and educate its students in these fast changing areas.

The school trains its staff to respond effectively to all online concerns and reports of cyber-bullying or harassment and has systems in place to respond to it. The school endeavours to block access to inappropriate websites, using firewalls, antivirus protection and filtering systems and no student is allowed to work on the internet in the Computer Room, or any other location within the school which may from time to time be used for such work, without a member of staff present.

Whilst education and guidance remain at the heart of what we do, we reserve the right to take action against those who take part in cyber-bullying, online hate, humiliation using AI or deepfakes. All bullying is damaging but cyber-bullying and harassment can always be invasive of privacy. These acts may also be criminal acts.

We support victims and, when necessary, will work with the Police to detect those involved in criminal acts. The school will use, as appropriate, the full range of sanctions to correct, punish or remove students who bully fellow students or harass staff in this way, both in and out of the school. The school will use its power of confiscation where necessary to prevent students from committing crimes or misusing equipment.

Cyber-bullying incidents are dealt with as bullying and safeguarding incidents and as such we follow the procedures outlined in our Behaviour for Learning Policy and Safeguarding and Child Protection policy.

Guidance for Staff

If a member of staff suspects or is informed about an online incident including cyber-bullying, they should follow the protocol outlined below:

- Report the incident to the DSL.
- Report the concern on CPOMS

If a student reports an incident on a school device. Secure the device, gather information from the student, report on CPOMS and inform your IT technician.

Guidance for Students

If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, or any trusted adult within the school.

Do not answer abusive messages but log and report them

Do not delete anything until it has been shown to your parents/guardian or trusted adult (even if it is upsetting as the material is important evidence which may need to be used later as proof of cyber-bullying)

- Do not give out personal IT details
- Never reply to abusive e-mails, messages or posts



- Never reply to someone you do not know
- Stay in public areas and do not private message

Guidance for Parents

It is vital that parents and the school work together to ensure that all students are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. The school informs parents of this policy and the procedures in place to deal with cyber-bullying. Parents can help by making sure their child understands the school's policy and, above all, how seriously it takes incidents of cyber-bullying.

Parents/Cares should also explain to their children legal issues relating to cyber-bullying. If parents/carers believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything. Parents/Carers should then contact the school as soon as possible.

Several sites offer helpful advice to parents/carers, particularly with respect to how they can best monitor their child's use of the computer at home. Important and useful information can be found on the following site:

- **UK Safer Internet Centre** – advice and resources for parents and carers to help children stay safe online.
- **Childline** – advice for children and young people about staying safe online.
- **NSPCC Online Safety** – guidance for parents and carers on keeping children safe online.
- **Internet Matters** – practical guidance for parents and carers on children's online safety and parental controls.
- **CEOP Education** – resources and advice about online sexual abuse and keeping children safe online.

Legal Issues

Cyber-bullying is generally criminal in character. It is unlawful to disseminate defamatory information in any media including internet sites. Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character. The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

9. Monitoring and Review

This policy will be reviewed annually or sooner in response to changes in national guidance. Behaviour data, safeguarding records and stakeholder feedback will inform evaluation of the policy's effectiveness.



Appendix 2: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) [glossary](#).

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Deep Fakes	Deep Fakes are digitally altered videos, images, or audio that falsely represent someone's actions or words.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.



TERM	DEFINITION
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

