



CEDARS ACADEMY TRUST

Cedars Academy: Low Fell
Cedars Academy: High Heworth

Online Safety and Acceptable Use of IT Policy

Policy owner	Director of Inclusion
Approved by	Curriculum & Pupils committee
Version	v1.0
Date approved	October 2026. Replaces the 2025-26 pupil acceptable use agreements.
Date written or last reviewed	September 2026
Next review due	September 2027
Status	Approved
Published on	Trust website and National College
Applies to	The Trust as a whole, across both sites

Index

The Policy

1. Purpose and scope	3
2. Legal framework	3
3. Roles and responsibilities.....	3
4. Online risks	4
5. Teaching online safety.....	4
6. Filtering and monitoring	4
7. Acceptable use of Trust IT.....	5
8. Staff, trustees and volunteers	5
9. Pupil agreements.....	6
10. Devices, searching and home use	6
11. Responding to concerns and misuse	6
12. Training	7
13. Monitoring and review	7

Appendices

Appendix 1: Pupil agreement, easy read version.....	8
Appendix 2: Pupil agreement, standard version.....	9
Appendix 3: Agreement for staff, trustees, volunteers and visitors	10
Annex A: Linked policies, forms and systems	11

The Policy

1. Purpose and scope

- 1.1** This policy sets out how the Trust keeps pupils, staff and trustees safe online, and how everyone must use the Trust's IT. It applies across the Trust, at Cedars Academy: Low Fell and Cedars Academy: High Heworth.
- 1.2** It applies to all pupils, staff, trustees, volunteers, contractors and visitors who use Trust IT. Trust IT means Trust devices (including iPads), the network and Wi-Fi, accounts, email, apps and online services, whether used on site, off site or at home. It also covers online behaviour outside school that affects pupils or staff.
- 1.3** Every pupil at the Trust has an Education, Health and Care Plan. Many of our pupils are more vulnerable online: they may be more trusting, find it hard to recognise risk, or be unable to tell us that something is wrong. Teaching, supervision and the pupil agreements are therefore adapted to each pupil's understanding.
- 1.4** Personal mobile phones and smartwatches are covered by the Mobile Phone Policy. Bullying, including online bullying, is covered by the Anti-Bullying Policy.

2. Legal framework

- 2.1** This policy follows Keeping Children Safe in Education 2026, which requires a whole-school approach to online safety and a review of filtering and monitoring at least once every academic year. It also follows the DfE filtering and monitoring standards (updated June 2026), Generative AI: product safety expectations, the cyber security standards for schools and colleges, Teaching online safety in schools, the statutory guidance on Relationships, Sex and Health Education, Searching, screening and confiscation, the UKCIS advice Sharing nudes and semi-nudes, and the Prevent duty guidance.
- 2.2** It reflects the law, including the Education Act 2011 powers to search devices and delete material, data protection law (UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025), the Computer Misuse Act 1990, the Online Safety Act 2023, the Equality Act 2010 and the Counter-Terrorism and Security Act 2015.

3. Roles and responsibilities

- 3.1** The Trust Board approves this policy and makes sure appropriate filtering and monitoring are in place and reviewed each year. Liz Neale is the trustee who leads on online safety and filtering and monitoring. Trustees sign the agreement at Appendix 3.
- 3.2** The three co-headteachers are jointly responsible for online safety across the Trust. Each site Headteacher makes sure this policy is followed at their site.
- 3.3** The Director of Inclusion, as Designated Safeguarding Lead, takes lead responsibility for online safety, including understanding the filtering and monitoring systems and acting on alerts. The Director of Inclusion is the senior leader responsible for filtering and monitoring.
- 3.4** The Academy Business Leader is responsible for the Trust's IT infrastructure and IT support contract, cyber security and data protection, working with the Trust's data protection officer. The Data and Office Manager manages the Trust's iPads through its mobile device management system, Mosyle.

- 3.5** The Trust's IT support provider, Omnicom, applies the filtering and monitoring settings, keeps systems secure and up to date, and manages user accounts.
- 3.6** All staff must read this policy, sign Appendix 3, supervise pupils' use of IT, teach and model safe behaviour, and report any online safety concern to the Designated Safeguarding Lead the same day.
- 3.7** Parents/carers are asked to sign their child's agreement, talk to their child about staying safe online, and tell the school about any concern.

4. Online risks

- 4.1** Online risks fall into four areas:
- content: seeing illegal, harmful or inappropriate material, such as pornography, violence, self-harm, extremism, misogyny or misinformation, including material created by AI
 - contact: harmful contact from others, including grooming, exploitation, adults posing as children, and AI chatbots that pretend to be a person
 - conduct: behaviour that causes harm, such as online bullying, or making or sharing nudes or semi-nudes, including fake images and deepfakes created with AI
 - commerce: scams, phishing, gambling and pressure to spend money, including financially motivated sexual extortion ('sextortion')

5. Teaching online safety

- 5.1** Pupils are taught about online safety through computing, Relationships, Sex and Health Education and PSHE, and whenever the chance arises in other lessons. Teaching is adapted to each pupil's understanding and communication, and repeated so that pupils can practise the skills.
- 5.2** Pupils are taught how to keep personal information private, how to tell a trusted adult when something online worries them, using their own way of communicating, that people and AI chatbots online are not always who they seem, and never to share images of themselves or others. Pupils are also taught, at a level they can understand, that convincing pictures, videos and voices can be fake, and how to seek help.
- 5.3** The Trust shares online safety information with parents/carers, including what filtering and monitoring is in place and how to set up controls at home.

6. Filtering and monitoring

- 6.1** Internet access on Trust devices and networks is filtered and monitored at both sites and on Trust devices used off site.
- 6.2** Filtering blocks illegal, harmful and inappropriate content, including AI-generated content, without unreasonably blocking learning. Monitoring alerts go to the Designated Safeguarding Lead, who acts on them.
- 6.3** Filtering and monitoring are reviewed at least once every academic year, and whenever new technology, including an AI tool, is introduced. The review is led by the senior leader responsible, with the Designated Safeguarding Lead and IT support. A record is kept of the checks made, the devices tested, any problems found and the action taken.

- 6.4** Staff must tell the Designated Safeguarding Lead if they, or a pupil, can see something that should be blocked, or if something needed for learning is blocked. Everyone who uses Trust IT is told that their use is monitored.

7. Acceptable use of Trust IT

- 7.1** Trust IT is for education and Trust work. Staff may make occasional personal use of it in their own time, away from pupils, provided the use is not unacceptable.

- 7.2** Unacceptable use of Trust IT, by anyone, includes:

- looking at, creating, storing or sharing illegal, pornographic, violent, extremist or discriminatory material
- bullying, harassing, threatening or humiliating anyone
- trying to get round filtering or monitoring, for example with a VPN or proxy
- using someone else's account, or sharing a password
- installing software or apps, or connecting a device, without approval
- looking at data without authority, or causing a data breach
- using an AI tool that the Trust has not approved, or putting personal or confidential information into any AI tool
- breaching copyright, damaging equipment on purpose, or running a private business

7.3 Artificial intelligence and manipulated content

- 7.31** AI can create or alter images, videos and audio, including making someone appear to say or do something they have not said or done. These are sometimes called 'deepfakes'.

No one may use AI or other editing tools to create, request or share content that bullies, humiliates, threatens, sexually exploits or harms another person, or impersonates them to mislead others. This includes fake nude or sexual images and tools that make a person appear undressed. Calling something a joke, or saying it is not real, does not make it acceptable.

Any permitted use of AI to create images, video or audio for learning or Trust work must use an approved tool and follow the Trust's data protection and image permissions requirements. Photographs, videos or voice recordings of pupils, staff or others must not be uploaded to an AI tool without specific Trust approval for that use. General permission to take or publish a photograph does not authorise its use in AI tools.

8. Staff, trustees and volunteers

- 8.1** Staff, trustees and volunteers must communicate with pupils and parents/carers only through Trust systems, such as Trust email and the parent communication app. They must never use a personal phone number, email address or social media account to contact a pupil or parent/carer, and must not connect with pupils on social media. Personal social media must be used in line with the Staff Code of Conduct.

- 8.2** Photos and videos of pupils must be taken only on Trust devices, only where parental consent for images is recorded, and stored only in Trust systems.
- 8.3** Trust data must be stored only in the Trust's approved systems. It must not be kept on personal devices or unencrypted memory sticks. Devices must be locked when not in use and protected by a strong password, with multi-factor authentication where available.
- 8.4** No AI tool is currently approved for use with Trust data. A tool may only be approved by the Academy Business Leader and the Designated Safeguarding Lead after a risk assessment against the DfE product safety expectations.
- 8.5** Staff must report a lost or stolen device, a suspected phishing email or a possible data breach to the Academy Business Leader straight away, so the Trust can meet its duty to report serious breaches to the Information Commission (the ICO) within 72 hours.
- 8.6** Trust devices taken home remain subject to this policy and must not be used by family members. Only staff authorised by the co-headteachers may post on the Trust websites or social media accounts.

9. Pupil agreements

- 9.1** Each pupil agrees to the version of the pupil agreement that matches their understanding. There are two versions. They are not tied to a pupil's age or site:
- the easy read version (Appendix 1) uses short, simple sentences and space for the pupil's own symbols
 - the standard version (Appendix 2) sets out the rules in full, for pupils who can read and understand them, with support if needed
- 9.2** The class teacher chooses the version with the pupil's parents/carers, taking account of the pupil's communication and understanding. The class team goes through it with the pupil using their preferred communication, such as symbols, signing or their AAC system. A pupil moves to the other version whenever that suits them better.
- 9.3** Where a pupil cannot understand either version, their parent/carer signs on their behalf, and staff keep the pupil safe through close supervision and device settings rather than relying on the agreement.
- 9.4** Agreements are signed when a pupil joins and at the start of each academic year, and kept on the pupil's record.

10. Devices, searching and home use

- 10.1** Pupils use Trust devices with their own login where they have one, under staff supervision. A pupil's communication aid is their voice: it is never removed as a sanction. Where it can access the internet, staff supervise its use.
- 10.2** The Headteacher, or a member of staff a Headteacher has authorised, may look at data on a device where there is a good reason, and may delete material that is not evidence of an offence, in line with Searching, screening and confiscation and the Behaviour Policy.
- 10.3** Where a device may hold a nude or semi-nude image of a child, staff must not view, copy, forward or delete it. They must secure the device and tell the Designated Safeguarding Lead at once.

- 10.4** Trust devices used at home remain filtered and monitored, and must not have these controls removed. Parents/carers should supervise their child's use at home.

11. Responding to concerns and misuse

- 11.1** Any online safety concern must be reported to the Designated Safeguarding Lead the same day and recorded on CPOMS. The Designated Safeguarding Lead decides the response under the Safeguarding and Child Protection Policy, including referral to children's social care, the police or Prevent where needed.
- 11.2** Online bullying is dealt with under the Anti-Bullying Policy. A concern about a member of staff's online conduct is dealt with under Part Four of Keeping Children Safe in Education 2026 and, where relevant, referred to the Local Authority Designated Officer.
- 11.3** Misuse by a pupil is dealt with under the Behaviour Policy, taking account of their SEND, and may include losing access to Trust IT for a time. Misuse by staff may lead to action under the Disciplinary Policy and Procedure. Anything that may be illegal is reported to the police.

12. Training

- 12.1** All staff receive online safety training at induction and regular updates, including how filtering and monitoring work and how to report concerns. Staff complete the cyber security training the Trust requires each year. Trustees receive online safety training as part of their safeguarding training. The Designated Safeguarding Lead updates their knowledge at least annually.

13. Monitoring and review

- 13.1** The Designated Safeguarding Lead keeps a record of online safety incidents on CPOMS and reports on them, and on the annual filtering and monitoring review, to the Trust Board (via Curriculum & Pupils committee) annually.
- 13.2** This policy is published on the Trust website and reviewed annually, or sooner if the law, guidance or technology changes.

Appendix 1: Pupil agreement, easy read & symbol version

Staying safe online

*For staff: go through this with the pupil using their own way of communicating. A symbol version is on the next page
Add the pupil's symbols in the left-hand column.*

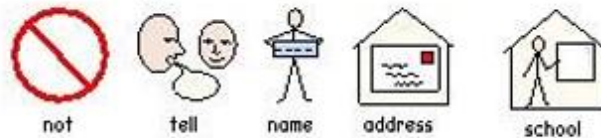
Symbol	What I will do
	I use the computer or iPad when an adult says I can.
	I only use apps and websites that adults say are OK.
	I keep my password secret, like my toothbrush. I do not use anyone else's.
	I do not tell people online my name, where I live or where I go to school.
	I am kind online.
	I tell an adult straight away if something online makes me sad, scared or worried.
	I tell an adult if someone online asks me to keep a secret or send a photo.
	I do not take photos or videos of people without asking an adult.
	I look after the computers and iPads. I tell an adult if something is broken.
	I do not change the settings.

If I break the rules, I might not use the computer or iPad for a while, and an adult will help me learn.

This is how we stay safe when we use computers:



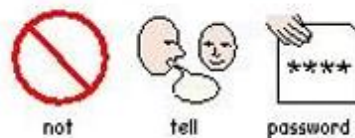
1. I **will not** share things about me or my family, like where we live, what clubs I go to or where I go to school.



2. I **will** tell an adult **straight away** if I see something that makes me feel bad or worried.



3. I **will** treat my username and password like my toothbrush – I will not share it and I will not use anyone else's.



4. I **will** be respectful, honest and kind when using the internet.



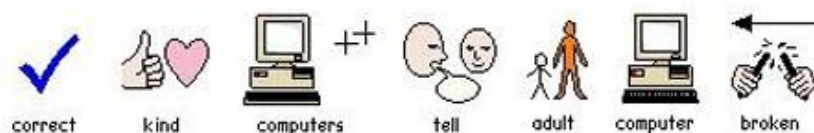
5. I **will not** write things about other people or take photos in school or on school trips to share on the internet.



6. I **will** only visit sites that adults in school say are ok.



7. I **will** look after the computer equipment in school and tell the teacher if it is broken.



8. I **will not** change any settings on the computers, laptops or tablets without my teacher's permission.



I know that if I break the rules I might not be allowed to use the computers at school.

Pupil name	
Pupil (name, mark or symbol)	
Parent/carer name and signature	
Staff member who went through this with the pupil	
Date	

Appendix 2: Pupil agreement, standard version

When I use the Trust's computers, iPads, internet and accounts, I will:

- use them only for learning, and only use the apps and websites that staff allow.
- use only my own username and password, keep my password secret, and log off when I have finished
- not try to get round the filtering, for example with a VPN, and not go into other people's files
- not look for, save or share anything unsuitable, and tell a member of staff straight away if I see something by accident
- not share personal information about myself or anyone else, and never arrange to meet someone I have met online
- tell a member of staff if anyone online makes me feel uncomfortable, asks me to keep a secret, or asks for photos
- be respectful online, and never bully, threaten or post anything hurtful
- not take or share photos or videos of anyone without their permission
- never make, ask for or share nude or semi-nude images, including fake images made with AI
- use AI tools only when staff allow, and not use them to hurt anyone or to pass off work as my own
- respect copyright and say where information comes from
- not install apps, change settings or plug in my own devices
- look after the equipment and report anything broken
- follow the Mobile Phone Policy

I understand that:

- the Trust checks how its IT is used, including Trust iPads used at home
- if I break these rules, I may lose access to the Trust's IT and other steps may be taken under the Behaviour Policy
- anything illegal may be reported to the police

Pupil name and signature	
Parent/carers name and signature	
Date	

Appendix 3: Agreement for staff, trustees, volunteers and visitors

I have read the Online Safety and Acceptable Use of IT Policy. When I use Trust IT, or any device for Trust business, I will:

- use Trust IT for Trust work, with only occasional personal use in my own time and away from pupils
- keep my passwords secret, use multi-factor authentication where available, and lock my device when I leave it
- store Trust data only in the Trust's approved systems, never on personal devices or unencrypted memory sticks
- communicate with pupils and parents/carers only through Trust systems
- take photos or videos of pupils only on Trust devices, and only where consent is recorded
- report any online safety concern about a pupil to the Designated Safeguarding Lead the same day
- report a lost device, suspected phishing or a possible data breach to the Academy Business Leader straight away
- supervise pupils' use of IT and tell the Designated Safeguarding Lead if filtering is not working

I will not:

- access, create or share illegal, pornographic, extremist or discriminatory material
- give pupils or parents/carers my personal phone number, email or social media details, or connect with pupils on social media
- try to get round filtering or monitoring, install software, or connect devices without approval
- put personal or confidential Trust information into any AI tool, or use an AI tool the Trust has not approved
- let anyone else use my account or a Trust device issued to me

I understand that the Trust monitors the use of its IT, and that breaking this agreement may lead to action under the Disciplinary Policy and Procedure or other Trust procedures, and to a report to the police if the law may have been broken.

Name	
Role (staff, trustee, volunteer, contractor or visitor)	
Signature	
Date	

Annex A: Linked policies, forms and systems

Linked policies

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Mobile Phone Policy
- Staff Code of Conduct
- Disciplinary Policy and Procedure
- Data Protection Policy
- RSE/RSHE Policy (site specific)
- Complaints Policy

Forms and systems

- CPOMS: online safety incidents and concerns
- Filtering and monitoring systems and the annual review record
- Mosyle: management of Trust iPads, maintained by the Data and Office Manager
- Signed pupil agreements (Appendices 1 and 2) and staff, trustee and volunteer agreements (Appendix 3)