



Online Safety Policy

2026–2027

*“From small beginnings come great things”
The Parable of the Mustard Seed — Matthew 13:31–32*

At Cadmore End we apply our Christian and British values, complemented by our small-school benefits, balancing each child’s educational, pastoral and emotional needs to deliver an exceptional, personalised experience that enables every child to flourish in our family and in the future.

Policy owner	Headteacher / Designated Safeguarding Lead
Approved by	Governing Board
Approval date	September 2026
Review date	July 2027
Responsible governor	Steve Kelsey

Policy statement

Online safety is an integral part of safeguarding, curriculum provision, behaviour, data protection and the responsible use of technology. The school recognises that technology provides valuable opportunities for learning and communication, while also creating risks that can arise inside or outside school and can move between online and offline environments.

Safeguarding principle

Any concern involving online behaviour, content, contact, technology or artificial intelligence will be considered first as a safeguarding matter. Staff must report concerns promptly to the DSL or a deputy and must never assume that another person has already done so.

1. Aims and scope

This policy applies to pupils, staff, governors, volunteers, contractors, visitors and other users of school systems. It applies to school-owned technology, personal devices used for school purposes, remote access, online services and online conduct that affects the safety or welfare of members of the school community.

The school aims to:

- protect pupils and adults from illegal, inappropriate and harmful online material and activity;
- educate pupils to use technology safely, respectfully, critically and responsibly;
- identify pupils who may be more vulnerable online and provide suitable, personalised support;
- maintain effective, proportionate filtering and monitoring without unreasonably restricting teaching and learning;
- establish clear arrangements to identify, record, respond to and escalate concerns;
- support parents and carers to understand online risks and the school's expectations; and
- promote a culture in which pupils confidently report concerns and know they will be listened to.

2. The four categories of online risk

Our whole-school approach addresses the four interrelated categories identified in Keeping Children Safe in Education 2026:

Content: Exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation, fake news, conspiracy theories and harmful challenges or hoaxes.

Contact: Harmful interaction with other users or generative AI applications that simulate interaction. This includes peer pressure, inappropriate advertising and adults posing as children or young adults to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: Online behaviour that causes or increases the likelihood of harm, including abusive, harassing, misogynistic or misandrist messages, online bullying, impersonation, non-consensual making or sharing of nudes or semi-nudes, and explicit images created or altered using AI.

Commerce: Online gambling, inappropriate advertising, phishing, scams, financial exploitation and other commercial risks.

3. Legislation and guidance

This policy has regard to relevant legislation and current national guidance, including:

- Keeping Children Safe in Education 2026 (DfE);
- Working Together to Safeguard Children;
- the Early Years Foundation Stage statutory framework;
- Teaching online safety in schools and the statutory relationships and health education guidance;
- the DfE filtering and monitoring core standard and cyber security standards;
- Searching, screening and confiscation: advice for schools;

- UKCIS Sharing nudes and semi-nudes: advice for education settings;
- Preventing and tackling bullying and the Prevent duty guidance;
- Mobile phones in schools guidance;
- the Education Act 1996, Education and Inspections Act 2006, Education Act 2011 and Equality Act 2010;
- the Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025; and
- the National Curriculum computing programmes of study.

4. Roles and responsibilities

4.1 Governing Board

The Governing Board has overall strategic responsibility for online safety and will hold the headteacher to account for implementation. It will:

- ensure appropriate safeguarding, filtering, monitoring, data-protection and cyber-security arrangements are in place;
- name a responsible governor and ensure a senior leader is responsible for meeting the filtering and monitoring standard;
- receive assurance that the annual filtering and monitoring review and risk assessment have been completed and actions addressed;
- ensure all staff receive appropriate induction, training and regular updates, including their roles in filtering and monitoring;
- ensure online safety remains an interrelated theme across safeguarding, curriculum, behaviour and staff conduct; and
- ensure provision is adapted for vulnerable pupils and pupils with SEND.

4.2 Headteacher

The headteacher is the senior leader responsible for the consistent implementation of this policy, for authorising personal devices for defined school purposes and for ensuring that resources, training and technical support are sufficient. Where the headteacher is also the DSL, the Governing Board and responsible governor provide appropriate challenge and oversight.

4.3 Designated Safeguarding Lead and deputies

The DSL has lead responsibility for safeguarding and online safety. The DSL will:

- understand the school's filtering and monitoring systems and review relevant reports and alerts;
- respond to safeguarding concerns identified by filtering and monitoring and escalate them appropriately;
- work with the headteacher, responsible governor and Classroom365 to review provision and risks;
- ensure online-safety incidents and decisions are recorded within the school's safeguarding system;
- coordinate support and risk assessment for affected pupils, including victims and pupils whose behaviour has caused harm;
- liaise with children's social care, police, CEOP, the local authority, Prevent/Channel or other agencies when required;
- provide regular assurance to governors and ensure lessons from incidents inform curriculum, training and technical controls; and
- maintain robust cover arrangements when the DSL is unavailable.

4.4 ICT support: Classroom365

Classroom365 has technical responsibility, within the agreed service arrangements, for maintaining filtering, monitoring and cyber-security systems; providing reports; completing checks and agreed technical actions; and advising the school about risks, limitations and system changes. Safeguarding decisions remain the responsibility of school leaders and the DSL.

4.5 Staff, volunteers and contractors

- read, understand and follow this policy, the staff code of conduct and the relevant acceptable-use agreement;
- use technology professionally and maintain confidentiality;
- understand how filtering and monitoring operate, remain vigilant and report failures or concerns immediately;
- never bypass controls unless an approved educational exception has been authorised and recorded;
- supervise pupils' technology use appropriately and teach safe practice whenever technology is used;
- respond to reports without blame or judgement and preserve evidence safely; and
- report concerns to the DSL or a deputy immediately, recording them through the school's safeguarding arrangements.

4.6 Pupils

Pupils will follow their age-appropriate acceptable-use agreement, treat others respectfully, protect personal information, use only approved services and report anything that worries, confuses, upsets or frightens them. Expectations will be explained and adapted so that pupils with SEND or communication needs can understand and participate.

4.7 Parents and carers

Parents and carers are asked to reinforce safe and respectful use, discuss the pupil agreement with their child and report concerns to the class teacher, headteacher or DSL. The agreement acknowledges shared expectations; it is not parental consent to opt out of statutory curriculum teaching.

5. Education and prevention

Online safety will be taught through computing, relationships and health education, PSHE and other subjects, and reinforced whenever pupils use technology. Teaching will be age appropriate, developmentally appropriate and revisited regularly. Pupils will learn:

- how online and face-to-face behaviour are connected, and how to be respectful and kind;
- how people may misrepresent themselves or use AI to simulate real people;
- how personal information, images and data are collected, shared, copied and used;
- how to recognise harmful content, contact, conduct and commercial pressure;
- how to evaluate reliability, recognise misinformation, disinformation and manipulated or AI-generated content;
- how to use strong, unique passwords and multi-factor authentication where provided;
- how online activity can affect mental and physical health, sleep, relationships and reputation;
- appropriate boundaries, consent and the risks of creating or sharing sexualised or intimate images;
- how to seek help, block or report content, preserve evidence safely and tell a trusted adult; and
- that they will be taken seriously and supported when they report a concern.

Teaching will be adapted for pupils who may be more vulnerable online, including those with SEND, communication needs, trauma, social-care involvement or limited understanding of risk. Adaptation will not reduce entitlement to essential safeguarding knowledge.

6. Engagement with parents and carers

The school will share relevant guidance through newsletters, the website, meetings and individual communication. Parents will be informed about the school's filtering and monitoring approach, what pupils are asked to access online and any significant emerging risks. The school may signpost the UK Safer Internet Centre, Childnet, CEOP Education and Internet Matters.

7. Filtering, monitoring and cyber security

The Governing Board and headteacher will ensure that filtering and monitoring are appropriate to the school's age range, pupil risk profile, SEND, curriculum, devices, locations and patterns of use. No system is completely effective; technical controls support, but do not replace, staff supervision and education.

The school will:

- identify a responsible SLT member and governor and document the responsibilities of the DSL, Classroom365 and other staff;
- complete and record a formal review at least once each academic year, involving the responsible SLT member, DSL, IT support and responsible governor;
- check that filtering operates on all school-managed internet-connected devices in all relevant locations and for the correct user groups;
- base the frequency of checks on risk and record when, by whom and what was tested, together with actions arising;
- review provision following a safeguarding risk, serious incident, new device or service, change in working practice, major software or configuration change, or introduction of generative AI;
- block illegal, harmful and inappropriate material without unreasonably affecting teaching and learning;
- use monitoring strategies that generate alerts or reports capable of timely safeguarding review;
- document filtering exceptions, why they are required, who authorised them and when they end; and
- protect accounts and information through appropriate access controls, updates, backups, encryption and incident response.

Reporting a failure

Any member of staff who believes filtering or monitoring has failed, has been bypassed or is preventing necessary learning must report it immediately to the headteacher, DSL or office manager. Staff must not attempt an unauthorised workaround.

8. Artificial intelligence

The school recognises the educational benefits and safeguarding, accuracy, bias, copyright and data-protection risks of generative AI. Only approved AI services may be used for school purposes and use must be appropriate to the age of the pupil and the provider's terms.

- Identifiable pupil, parent, staff, safeguarding or other confidential information must not be entered into an unapproved AI system.
- AI output must be checked by a competent adult; professional judgement and responsibility cannot be delegated to AI.
- New AI products or materially new uses must undergo proportionate safeguarding, privacy and product-safety assessment before use.
- Pupils will be taught that AI output may be inaccurate, biased, fabricated or manipulative and must not be treated automatically as a reliable source.
- AI-generated bullying, impersonation, sexualised imagery, deepfakes and deep nudes will be treated as serious safeguarding matters.
- Filtering and monitoring reviews will consider dynamic, personalised and AI-generated content and any technical limitations.

9. Online bullying and child-on-child abuse

Online bullying includes harmful behaviour through messaging, gaming, social media, shared documents, images, video, impersonation or other digital services. Bullying is commonly repetitive and involves an imbalance of power; however, a serious one-off online incident will still be addressed and may constitute a safeguarding concern or child-on-child abuse.

Reports will be handled under the child-protection and behaviour procedures. The school will consider the needs and wishes of the child affected, the risk to others, support for all involved, appropriate sanctions, parental involvement, evidence preservation and referral to external agencies.

10. Sharing nudes and semi-nudes and illegal content

A staff member who becomes aware that a device may contain a nude or semi-nude image of a child, including an AI-generated or digitally altered image, must not view, copy, print, forward, save, ask a pupil to share or delete it, or investigate the matter personally. The device should be secured without searching it and the DSL informed immediately. The DSL will follow the current UKCIS guidance and seek police or children's social-care advice where required.

Suspected child sexual abuse material must never be emailed, uploaded, printed or otherwise reproduced. Staff will preserve the device and relevant contextual information and follow agency advice. Other suspected illegal or harmful content will be escalated to the DSL, who will determine the appropriate reporting route.

11. Searching and confiscating electronic devices

Only the headteacher or a member of staff authorised by the headteacher may search a pupil or confiscate and examine a device, and only in accordance with current DfE searching, screening and confiscation guidance and the school's behaviour policy. Before any search, the member of staff will consider urgency, safeguarding risk, the pupil's cooperation and whether advice from the DSL is required.

Data will not be deleted where it may be evidence of an offence or safeguarding concern. If a search might expose staff to indecent imagery of a child, the procedure in section 10 applies. Any search, examination, deletion decision and action will be proportionate and recorded.

12. Pupil mobile phones, smartwatches and connected devices

Pupils may not bring a mobile phone, smartwatch or other personally connected device to school unless the headteacher has granted permission because of a specific need or family arrangement. Approved devices must be switched off, handed to or stored as directed by the school, and not used during the school day without staff permission.

- Parents and carers should contact pupils through the school office during the school day.
- Reasonable adjustments or individual arrangements may be agreed for medical, SEND or safeguarding reasons.
- Trip and residential arrangements will be explained separately and will remain consistent with safeguarding expectations.
- Unauthorised use will be addressed proportionately under the behaviour policy; confiscation will follow statutory guidance.
- The school accepts no responsibility for loss or damage except where liability arises through the school's own actions.

13. Staff devices, photography and recordings

13.1 Work devices

- Work devices must be password or passcode protected, encrypted where supported, locked when unattended and kept up to date.
- Devices must not be shared with family or friends and school information must only be stored or transferred through approved systems.
- Loss, theft, suspected compromise or a data breach must be reported immediately to the headteacher, DSL and DPO as appropriate.
- Work devices are for authorised professional use and must comply with the acceptable-use agreement and staff code of conduct.

13.2 Authorised use of personal phones for school photographs

The headteacher and specifically authorised members of staff may use a personal mobile phone to take photographs or recordings of pupils for an approved educational or school purpose. Authorisation will be recorded by the school, reviewed periodically and may be withdrawn.

Authorised staff must:

- check that the image is necessary and permitted by the school's consent and privacy arrangements;
- use the device's standard camera and not capture or store images through personal social-media or messaging applications;
- avoid recording more personal information than is necessary;
- transfer the image promptly to the school's approved secure storage or communication system;
- delete it immediately after transfer or authorised use, including from "recently deleted" and any personal cloud backup;
- never retain, privately share, edit or use the image for another purpose; and
- report loss, accidental sharing, suspected breach or safeguarding concerns immediately.

Where the headteacher or DSL has a reasonable safeguarding or data-protection concern, an authorised staff member may be required to produce the relevant school-related images and associated information for review. Any review will be proportionate, limited to the school-related concern and handled sensitively to respect personal privacy.

Personal devices must not normally be used to photograph injuries, intimate care, suspected abuse or material that may constitute illegal imagery. The DSL must be consulted and safeguarding procedures followed.

14. Responding to incidents

The immediate priority is safety and welfare. Staff will:

- listen calmly, take the report seriously, avoid blame and avoid promising confidentiality;
- not investigate beyond what is necessary to establish an immediate safeguarding response;
- report promptly to the DSL or deputy and record the child's words, context and immediate action;
- preserve evidence without copying or unnecessarily viewing harmful material;
- consider immediate protection, medical needs, risk to other children and support for all affected pupils; and
- follow child-protection, behaviour, data-protection, complaints, staff-conduct or disciplinary procedures as applicable.

The DSL will decide whether to refer to children's social care, police, CEOP, Prevent/Channel, the local authority, the DPO/ICO or another agency. Incidents involving staff will be managed under the allegations or low-level-concerns procedures and referred to the local authority designated officer where the threshold is met.

15. Recording, monitoring and review

Safeguarding-related online-safety incidents will be recorded in the school's safeguarding recording system. Technical logs or the form in Appendix 4 may support the record but do not replace it. Records will include the concern, child's voice where relevant, decisions, risk assessment, referrals, support, outcomes and lessons learned. Personal data breaches will also follow the school's data-breach procedure.

The headteacher and DSL will monitor themes and report appropriately to governors without unnecessary personal information. This policy will be reviewed at least annually and sooner following significant guidance changes, incidents, identified risks or changes in technology or school practice.

16. Training

All staff will receive online-safety and filtering-and-monitoring training at induction, regularly updated safeguarding training and updates as required and at least annually. DSLs and deputies will receive training appropriate to their role and update their knowledge at least annually. Governors will receive appropriate safeguarding and online-safety training. Volunteers and contractors will receive information proportionate to their role.

17. Related policies and procedures

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection Policy, privacy notices and data-breach procedure
- Anti-bullying arrangements
- Complaints Procedure
- Searching, Screening and Confiscation arrangements
- Remote-learning arrangements, where applicable
- Curriculum policies for computing, relationships and health education and PSHE

Appendix 1: EYFS and Key Stage 1 pupil agreement

My safe technology promises

An adult will explain these promises to me in a way I understand. I can use words, pictures, signs or another way of communicating to show that I understand.

- I will ask an adult before I use school technology or go online.
- I will use only the apps, websites and activities an adult has chosen.
- I will be kind and respectful when I use technology.
- I will keep personal information and passwords private.
- If I see or hear something that worries, frightens or upsets me, I will stop and tell a trusted adult.
- I will tell an adult if somebody online asks me to do something that feels wrong or secret.
- I will look after school equipment and tell an adult if something is broken.
- I know I will not be in trouble for asking for help.

Pupil's name	
How the agreement was explained	
Pupil acknowledgement	
Date	

Parent/carers acknowledgement: I have discussed these expectations with my child in a way they can understand and will support safe, respectful use of technology.

Parent/carers name and signature	
Date	

Appendix 2: Key Stage 2 pupil agreement

When I use school technology, school accounts or the internet for school work, I will:

- use technology only for an agreed educational purpose and follow staff instructions;
- be kind, respectful and responsible and never use technology to bully, embarrass, threaten or impersonate somebody;
- keep passwords private, use my own account and tell an adult if I think an account is unsafe;
- protect personal information about myself and others, including names, addresses, locations, photographs and contact details;
- ask permission before taking or sharing a photograph, recording or somebody else's work;
- think critically about whether online information or AI output is accurate, fair and trustworthy;
- not try to bypass filtering, change settings, install software or access another person's files;
- not open unexpected links or attachments and tell an adult about suspicious messages;
- stop and tell a trusted adult if I see or receive anything worrying, harmful, sexual, frightening or confusing;
- never create, request or share nude, semi-nude, sexualised or humiliating images, including images made or changed using AI;
- not arrange to communicate privately or meet with someone first known online without involving my parent or carer; and
- understand that the school filters and monitors use of its devices, accounts and networks to help keep everyone safe.

Pupil's name and signature	
Parent/carers acknowledgement	
Date	

Appendix 3: Staff, governor, volunteer, contractor and visitor agreement

I will use school systems, information and technology lawfully, safely and professionally. I will:

- protect passwords and accounts, use multi-factor authentication where provided and change a password immediately if compromise is suspected;
- access only information and systems required for my authorised role;
- use approved communication, storage and sharing systems and protect confidential information;
- not use personal email, personal cloud storage or personal messaging services for school information;
- not communicate privately with pupils through personal accounts, numbers or social media;
- not install unauthorised software, connect unauthorised hardware or attempt to bypass filtering or monitoring;
- report safeguarding concerns, filtering failures, suspicious messages, loss, compromise and data breaches immediately;
- follow the authorised-personal-phone photography procedure in section 13.2 where it applies to me;
- not enter identifiable or confidential school information into an unapproved AI service and verify any AI-assisted work;
- maintain appropriate professional boundaries and ensure pupils in my care use technology safely; and
- understand that authorised use of school devices, accounts and networks is logged and monitored proportionately for safeguarding, security and compliance.

Name	
Role	
Signature	
Date	

Appendix 4: Online-safety incident record

Use this form only where it supports the school's safeguarding or technical record. Safeguarding concerns must also be entered in the school's safeguarding recording system.

Date and time	
Pupil(s)/person(s) involved	
Where and how concern arose	
Factual description, including child's words	
Immediate safety action	
Evidence secured and where held	
DSL informed: name/time	
Risk assessment and support	
Parents/carers informed or reason not informed	
External referral/advice	
Technical action, including filtering changes	
Outcome, review and lessons learned	
Recorded by/signature/date	

Appendix 5: Annual filtering and monitoring review record

Review area	Evidence, findings and actions
Review date and participants	Include responsible SLT member, DSL, Classroom365/IT support and responsible governor.
School risk profile	Age range, SEND/EAL, vulnerable groups, curriculum, safeguarding themes and outside influences.
Devices, services and locations	Confirm all school-managed internet-connected devices, accounts, networks and relevant locations.
What is blocked and allowed	Record categories, user groups, exceptions, limitations and impact on teaching and learning.
Monitoring strategy	Alerts/reports, recipients, review frequency, response arrangements and cover.
Checks completed	Record date, tester, devices/locations/user groups tested, results and evidence.
AI and dynamic content	Record products in use, risk assessment, filtering/monitoring capability and limitations.
Incidents and intelligence	Themes, serious incidents, near misses, pupil voice, staff concerns and lessons learned.
Training and curriculum	Staff understanding, pupil learning and parent/carers engagement.
Actions, owner and deadline	List each gap or improvement, accountable owner, completion date and evidence.
Governor assurance	Responsible governor review, challenge and date reported to the Governing Board.