CUBITT TOWN PRIMARY SCHOOL

Online Safety Policy

2026–27

Every child grows • Every voice matters • Every day counts

This policy applies to all staff, pupils, parents and carers, governors, volunteers, contractors and visitors

Headteacher	Robyn Bruce
Designated Safeguarding Leads	Robyn Bruce, Karen Ward, Jacqui Jenkins
Deputy DSLs	Angie Drew, Rabia Begum
Online safety lead	Shehan Wijayaratne
Computing lead	Shehan Wijayaratne
PSHE / RSHE lead	Fatima Begum
Senior leader for filtering and monitoring	Jacqui Jenkins/Karen Ward
IT support / network manager	Afzal /Connetix
Data Protection Officer	Noamo
Safeguarding and online safety link governor	Margaret Davies
Date approved	September 2026
Next review	Autumn 2027, or sooner if needed

Contents

1. Our vision, values and online safety
2. Aims and scope
3. The main online safety risks
4. How this policy is communicated
5. Roles and responsibilities
6. Education and curriculum
7. Handling online safety concerns and incidents
8. Filtering and monitoring
9. Data protection and data security
10. Email and electronic communications
11. School website and cloud platforms
12. Digital images and video
13. Social media
14. Mobile phones and personal devices
15. Searching and confiscation
16. Related policies and monitoring

1. Our vision, values and online safety

At Cubitt Town Primary School, **together we strive for excellence**. Technology opens up a world of learning, creativity and connection for our children, and we want every child to enjoy it safely, confidently and kindly – both in school and at home. Online safety is part of safeguarding, and it is everyone's responsibility.

Every child grows	Every voice matters	Every day counts
Every child learns, step by step from Nursery to Year 6, the knowledge and skills to use technology safely, think critically about what they see online, and make good choices.	Children know they can always tell a trusted adult – or use Toot Toot or a worry box – if something online worries them, and they will be listened to without blame.	Adults are vigilant every day, supervise online learning closely, and act on any concern the same day.

Our 6C values online

Value	What it means online
Care	We are kind online, look after our personal information and our wellbeing, and look out for others.
Communication	We speak respectfully online, and we tell a trusted adult straight away if we see or experience something that worries us.
Collaboration	School and families work together to keep children safe online, sharing advice and concerns.
Curiosity	We ask questions about what we see online: Is it true? Who made it? Why? – including content made by AI.
Challenge	We challenge unkind behaviour, bullying, prejudice and misinformation online, and we have the confidence to say no.
Commitment	We follow our acceptable use agreements every time we use technology, in school and at home.

2. Aims and scope

This policy aims to:

- set out expectations for the online behaviour and use of digital technology of everyone in the Cubitt Town community, including when devices are offline;
- help everyone understand that standards of online behaviour, including on social media, apply beyond the school gates and school day, whatever the device or platform;
- support the safe, responsible and respectful use of technology for teaching and learning, preparing children for the risks and opportunities of today's and tomorrow's digital world;
- help staff understand their roles and responsibilities for working safely with technology – to protect children, to protect themselves from misplaced or malicious allegations, and to protect the reputation of the school;
- set out clear procedures for responding to online safety concerns, alongside our Safeguarding and Child Protection, Behaviour Regulation and Anti-bullying policies.

This policy applies to all members of the Cubitt Town Primary School community – staff, governors, volunteers, contractors, pupils, parents and carers, visitors and community users – who have access to our digital technology, networks and systems, whether on site or remotely, or who use technology in their school role.

3. The main online safety risks

Keeping Children Safe in Education (KCSIE) 2026 groups online safety risks into four areas – the **4 Cs**. They often overlap:

- **Content:** being exposed to illegal, inappropriate or harmful material, such as pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism, and **misinformation, disinformation (including fake news) and conspiracy theories**.
- **Contact:** being subjected to harmful online interaction with other users, such as peer pressure, commercial advertising, and adults posing as children to groom or exploit them.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm – for example, making, sending and receiving explicit images, and online bullying.
- **Commerce:** risks such as online gambling, inappropriate advertising, in-game purchases, phishing and financial scams.

Generative artificial intelligence (AI) brings new opportunities and new risks, including AI-generated sexual images of children ('deepfakes'), realistic misinformation, and chatbots that are not designed for children. We follow the DfE's guidance on generative AI in education and its product safety expectations when considering any AI tool.

4. How this policy is communicated

- Published on the school website and saved in the policies folder on the staff shared drive.
- Part of the induction pack for all new staff, including temporary, supply and non-classroom-based staff, volunteers and governors.
- Covered in safeguarding training and updates for all staff, especially the September refresher.
- Reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents and carers. AUPs are signed on joining the school, with annual reminders, and reissued when updated.
- Child-friendly AUPs and online safety rules are displayed in every classroom and next to computers.
- Reviews of this policy include the views of staff, pupils and parents.

5. Roles and responsibilities

Our school is a community, and everyone has a duty to behave respectfully online and offline, to use technology for learning, and to report any concern or inappropriate behaviour immediately. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher – Robyn Bruce

- Foster a culture in which online safety is fully part of whole-school safeguarding.
- Oversee and support the DSLs, and make sure policies and procedures are followed by all staff.
- Undertake safeguarding training, including online safety, in line with statutory guidance and THSCP arrangements.
- Take overall responsibility for data protection and information security, working with the DPO, DSLs and governors.
- Make sure the school uses appropriate IT systems, including school-safe filtering and monitoring, secure email and cloud systems implemented on child-safety-first principles.
- Make sure all staff receive suitable training and know what to do in a serious online safeguarding incident.
- Make sure risk assessments are carried out, including the Prevent risk assessment, and that staff carrying out technical online safety procedures are supported and monitored.
- Keep governors informed about online safety, and make sure the school website meets statutory requirements.

Designated Safeguarding Leads (with the Online Safety Lead)

- Take lead responsibility for online safety, as set out in KCSIE 2026.
- **Filtering and monitoring:** understand and make sure the school's filtering and monitoring systems are effective and meet the DfE filtering and monitoring standards; work with the senior leader for filtering and monitoring and IT support to review and test them at least annually; and respond to monitoring alerts and reports.
- **Generative AI:** make sure filtering, monitoring and risk assessments take account of AI tools, and that any AI tool used meets DfE product safety expectations.
- **Policy and training:** keep this policy and the Safeguarding Policy up to date with the latest guidance, including misinformation, disinformation and conspiracy theories; make sure all staff receive regular online safety training and induction, read KCSIE Part 1 (and Annex A where appropriate), and are aware of the online safety content of KCSIE.
- **Coordination:** assess online safety risks in our context; work with the Computing and PSHE/RSHE leads so that digital literacy and critical thinking are taught well; be the clear contact for online safety concerns; and give governors assurance that systems work well.
- Record online safety concerns on CPOMS and refer to MAST, the police or other agencies as needed.

Governing Body – led by the Safeguarding Link Governor, Margaret Davies

- Make sure the school meets its statutory duties, including having appropriate filtering and monitoring in place and reviewed at least annually.
- Scrutinise this policy, the Safeguarding Policy and the Staff Code of Conduct to check they reflect current risks, such as cyberbullying, child-on-child abuse, misinformation and generative AI.
- Seek assurance about filtering and monitoring: how effectiveness is measured, how alerts are escalated, and how AI tools and pupil data are protected.
- Check that online safety is taught progressively across all year groups, including how pupils learn to question what they see online.

- Make sure staff and governors receive regular, up-to-date training; meet regularly with the DSLs and Headteacher; and report to the full Governing Body.

All staff

- Understand that online safety is a core part of safeguarding and part of everyone's job – never assume someone else will deal with it.
- Know who the DSLs are; read KCSIE Part 1 (and Annex A where appropriate) and this policy alongside the Safeguarding Policy.
- Record and report online safety concerns on CPOMS in the same way as any other safeguarding concern – the same day, and immediately if urgent. Safeguarding is like a jigsaw: you may have the missing piece.
- Sign and follow the staff AUP and Staff Code of Conduct.
- Supervise pupils closely whenever they use technology, check websites and resources before using them, and support pupils with search skills, critical thinking, age-appropriate content and copyright.
- Look for opportunities to teach online safety across the curriculum and in unexpected moments.
- Tell the DSL about new trends and issues, and take a zero-tolerance approach to bullying and sexual harassment, online and offline.
- Be aware that online issues are often seen or overheard in the playground, corridors and other shared spaces.
- Model safe, responsible and professional use of technology, including outside school and on social media.

PSHE / RSHE Lead

- Make sure the Relationships and Health Education curriculum meets the DfE statutory guidance (in full from September 2026), including respectful online relationships, recognising harmful content and contact, privacy settings, age limits for social media, online gaming, scams and wellbeing online, and where to get help.
- Work with the DSL and Computing Lead to teach media literacy and critical thinking, including about misinformation, misogynistic content and the responsible use of AI.
- Consult parents and carers on the curriculum and share teaching materials openly.
- Link with the DSL and Attendance Lead, recognising that emotional health and knowing where to get help are part of our preventative work.

Computing Lead and subject leaders

- Oversee the online safety element of the Computing curriculum, in line with the National Curriculum.
- Work with the DSL, IT support and all staff so that messages about online safety are consistent.
- Use the UKCIS framework Education for a Connected World and the DfE's Teaching Online Safety in Schools to plan progression, including for pupils with SEND.
- Make sure subject action plans include online safety where relevant.

Network manager / IT support – Afzul – Connetix

- Keep up to date with this policy and technical guidance, and work with the DSLs, the DPO and the Headteacher so that systems reflect school policy.
- Explain the impact of any changes to systems, such as filtering settings, YouTube restricted mode or sharing permissions on cloud platforms.
- Support the implementation and annual review of filtering and monitoring, and keep records of checks.
- Manage systems, networks and devices securely – strong passwords, multi-factor authentication, anti-virus and anti-phishing protection, encryption, backups and disaster recovery – in line with the DfE digital and technology standards, including the cyber security standards.

- Report online safety issues in line with school policy, and help make sure the website meets DfE requirements.

Data Protection Officer

- Work with the Headteacher, DSLs and governors to make sure data is protected, while making sure data protection never stands in the way of keeping children safe.
- Advise on data protection impact assessments (DPIAs) for new systems, including AI tools and cloud platforms.
- Make sure access to safeguarding data is limited, monitored and audited, and that records are kept in line with the school's retention schedule.

Volunteers and contractors

- Read, sign and follow the relevant AUP.
- Report any concern, however small, to a DSL.
- Model safe, responsible and professional use of technology, and never use personal devices to photograph children.

Pupils (in an age-appropriate way)

- Learn and follow our class online safety rules and pupil AUP.
- Know that they can tell a trusted adult, use Toot Toot or a worry box if they, or a friend, see or experience something that worries them online.
- Understand that our online safety rules and values apply at home too, including on games, apps and social media.
- Understand the good things about the online world, as well as the risks, and know who to talk to in and out of school.

Parents and carers

- Read and sign the parent AUP, and help their child understand and follow the pupil AUP.
- Talk to the school if they have any concerns about their own or other children's use of technology.
- Model safe and positive use of technology, including on social media: not sharing other people's images or details without permission, and not posting negative or threatening comments about staff, pupils or other families.
- Talk regularly with their child about the apps, sites and games they use, and use parental controls and age ratings.

6. Education and curriculum

Online safety is taught through Computing, PSHE and Relationships and Health Education, and threaded through the whole curriculum. Our teaching follows the UKCIS framework **Education for a Connected World** – covering self-image and identity, online relationships, online reputation, online bullying, managing online information, health and wellbeing, privacy and security, and copyright and ownership – and is adapted for pupils with SEND and pupils learning English.

At Cubitt Town:

• Children learn about online safety from the Early Years, starting with simple messages such as asking an adult before using a device and telling an adult if something upsets them.

• Our oracy approach gives children the language to discuss online dilemmas, question what they see, and explain their choices.

• We mark Safer Internet Day each year, and hold online safety assemblies.

• Resources are adapted for pupils with SEND, using visuals and Widgit symbols.

• We share online safety guidance with families on Class Dojo and the website, and run online safety workshops for parents.

Whenever pupils use technology, staff supervise closely, encourage sensible use, monitor what pupils are doing, and consider the age-appropriateness of websites and apps.

7. Handling online safety concerns and incidents

Online safety is part of safeguarding. Online safety concerns are handled in the same way as any other safeguarding concern, in line with our **Safeguarding and Child Protection Policy**, and also our Anti-bullying Policy, Behaviour Regulation Policy, Acceptable Use Policies, Prevent risk assessment and Data Protection Policy.

We take all reasonable precautions to keep everyone safe online, but recognise that incidents will happen both in and outside school, and that incidents outside school affect children when they come to school.

- Any online safety concern about a child must be recorded on **CPOMS** and reported to a DSL the **same day** – and immediately if a child is at risk of harm.
- Any concern or allegation about the conduct of a member of staff online is reported to the Headteacher, or to the Chair of Governors if it concerns the Headteacher, in line with our Whistleblowing Policy and the LADO procedures. Staff can also use the NSPCC Whistleblowing Helpline (0800 028 0285).
- The school will seek support from other agencies where needed, including MAST, the police, the local authority, the UK Safer Internet Centre's Professionals Online Safety Helpline, CEOP, the Prevent team and the Internet Watch Foundation.
- We will tell parents and carers about online safety incidents involving their child, unless the DSL decides this would put the child at risk, and we will involve the police where behaviour breaks the law or is particularly concerning.

Sharing nudes and semi-nudes (youth-produced sexual imagery)

We follow the UKCIS guidance **Sharing nudes and semi-nudes: advice for education settings** (updated March 2024). All staff know that if they become aware of an incident they must **not view, copy, share or delete the image, or ask anyone else to do so** – they go straight to a DSL, who will follow the guidance and decide whether other agencies need to be involved. This includes images altered or created using AI. Children are reassured that they can talk to an adult if they have made a mistake or had a problem. Where one of the people involved is an adult, this is child sexual abuse and will be referred immediately.

Upskirting

Upskirting – taking a photo under someone's clothing without their permission – is a criminal offence. Any report will be passed to a DSL. Children know they can talk to staff if something has happened.

Online bullying

Online bullying (cyberbullying) is treated like any other form of bullying, in line with our Anti-bullying Policy and our restorative approach, including the Cubitt Town Peace Path.

Sexual violence and sexual harassment

Any incident of sexual harassment or sexual violence, online or offline, is reported to a DSL, who will follow KCSIE 2026 Part 5 and our Safeguarding Policy. Staff maintain a zero-tolerance culture and never dismiss behaviour as 'banter'.

Misuse of school technology

Rules for using school networks, devices, cloud platforms and social media are set out in our AUPs and this policy. Where pupils break these rules, our Behaviour Regulation Policy is followed; where staff do so, the Staff Code of Conduct applies. The school may withdraw access to technology, temporarily or permanently.

Social media incidents

Breaches of our social media expectations are dealt with under the Behaviour Regulation Policy (pupils) or the Staff Code of Conduct (staff). Where a member of the school community posts something inappropriate, upsetting, violent or abusive, the school will ask for it to be deleted promptly. Where a post is made by a third party, we may report it to the platform and seek help from the Professionals Online Safety Helpline.

8. Filtering and monitoring

KCSIE 2026 requires the school to have appropriate filtering and monitoring, so that children cannot access harmful or inappropriate material, while making sure that 'over-blocking' does not lead to unreasonable restrictions on what children can be taught. We meet the DfE filtering and monitoring standards by:

- identifying and assigning roles and responsibilities for managing filtering and monitoring (see the cover page);
- reviewing the effectiveness of our filtering and monitoring at least annually – led by the senior leader responsible, with the DSL and IT support – and keeping records of reviews and checks;
- blocking harmful and inappropriate content without unreasonably affecting teaching and learning;
- having effective monitoring strategies that meet our safeguarding needs.

At Cubitt Town, our internet is provided by LGFL and filtered using LGFL webscreen Monitoring is provided through SENSO with alerts sent to the DSLs and followed up the same day.

We use three types of monitoring: **physical monitoring** (adults supervising children whenever they use technology), **internet and web access logs**, and **active technology monitoring**.

Staff report any website or content that should be blocked, or any over-blocking, to IT support / online safety lead.

9. Data protection and data security

Data protection legislation – the Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025 – **does not prevent or limit the sharing of information to keep children safe**. Safeguarding is a lawful reason to share sensitive information, even without consent where seeking consent would put a child at risk. Fears about sharing information must never stand in the way of protecting children. The DSLs record what information they share, with whom and why.

- All staff, governors, volunteers and contractors are bound by the school's Data Protection Policy.
- Safeguarding information is highly sensitive: it is stored on CPOMS, and shared only through approved, secure channels with those who need it.
- Pupil data is never sent by personal email or stored on personal devices. Personal data sent outside the school is sent using [secure/encrypted email system, e.g. Egress].
- The school meets the DfE's cyber security standards, including strong passwords, multi-factor authentication, staff training on phishing, and secure backups.

10. Email and electronic communications

- Staff use their school Google Workspace account for all school email. Personal email is never used for school business; if this happens by mistake, the DSL, Headteacher or DPO must be told immediately.
- School email and systems may be monitored, and must not be used to send anything that is, or could be seen as, bullying, aggressive, rude, illegal or unprofessional.
- Remote learning uses Google Classroomwith school accounts only. Staff never use personal accounts to contact pupils.
- **Class Dojo** is our main channel for messages between school and parents and carers; general enquiries can also go to the school office by email or phone.

11. School website and cloud platforms

Our website is our main public source of information and is hosted by De Beers The Headteacher and Deputy Headteacher are responsible for keeping it up to date and making sure it meets DfE requirements. Anyone adding content must respect copyright and must never publish pupils' full names alongside their photos.

Before any new cloud platform or app is introduced, the DPO and IT support check it, a data protection impact assessment is completed where needed, and parents are informed. Only school-approved platforms are used to store pupil work and data. Multi-factor authentication is used for systems holding staff or pupil data, staff are trained in sharing settings, and everyone understands the difference between personal and school accounts.

12. Digital images and video

- When a child joins the school, parents and carers are asked for consent for their child's image to be used, and for what purposes (for example, displays and newsletters, the website, and social media). Staff check consent on Arbor before using any image.
- Pupils in public-facing materials are identified by first name only, if at all, and file names never include full names.
- Staff take photos and videos of pupils **on school devices only** unless agreed by the HT. Images are stored on the school network or approved cloud storage, in line with the retention schedule.
- Children who are looked after, or who have other reasons, may have restrictions on their image being used; staff check before sharing any image.
- Parents and carers are asked not to share photos or videos of other children from school events on social media.
- Children learn how images can be manipulated or created with AI, to ask permission before taking or sharing images of others, and to protect their own privacy.

13. Social media

The school's social media

The school's official social media account ([X / Instagram – @CubittTownPri]) is managed by Shehan Wijayratne We monitor our online presence and respond to comments fairly and responsibly. Parents and carers are asked not to use social media to communicate with the school about their child.

Staff, pupils and parents

- Everyone is expected to behave positively and respectfully on social media, in the same way as they would face to face – on public pages and in private groups and parent chats.
- If parents or carers have a concern about the school, they should speak to us directly so that we can resolve it, using our Complaints Procedure if needed – not post it on social media.
- Many social media platforms have a minimum age of 13. We ask parents to respect age ratings and not encourage underage use, but our lessons help children know how to stay safe and report problems if they do use apps and games.
- Pupils must not be 'friends' with, or send friend requests to, staff, governors, volunteers or contractors, and staff must never follow or contact pupils on social media. Any exceptions (for example, family links) must be declared to and approved by the Headteacher. Any attempt to do so will be reported to a DSL (if by a child) or to the Headteacher (if by an adult).
- Staff must use strict privacy settings, never discuss the school, pupils or families on social media, and never bring the school or profession into disrepute.

14. Mobile phones and personal devices

In line with the DfE guidance **Mobile phones in schools** (February 2026) and our Mobile Phone Policy:

- **Pupils** may not use mobile or smart phones or smart watches with cameras or messaging during the school day. We encourage families not to give children phones before Year 6, and in Year 6 only if they travel to and from school on their own. Any phone brought to school is handed in at the start of the day and collected at the end.
- **Staff** keep personal phones on silent and away from children, and use them only in designated areas and at break times, or in an emergency. Staff never use personal devices to photograph pupils or store pupil data. Urgent personal calls can be taken through the school office.
- **Volunteers, contractors and governors** keep phones away and switched off around children, and never take photos or videos without the Headteacher's permission and a member of staff present.
- **Parents and carers** keep phones away when on site, ask permission before taking photos (for example of displays), and avoid capturing other children.
- On **trips**, staff use a school phone where possible. If a personal phone is used in an emergency, the number is withheld.
- The school's guest Wi-Fi is available to approved visitors only, is filtered and monitored, and gives no access to school files.

15. Searching and confiscation

In line with the DfE guidance **Searching, screening and confiscation** (July 2022), the Headteacher and staff authorised by them have a statutory power to search pupils and their possessions, including electronic devices, where there are reasonable grounds to suspect they contain something prohibited or harmful. Staff must never view, copy or delete suspected nude or semi-nude images – these are passed to a DSL, in line with the UKCIS guidance. Full details are in our Behaviour Regulation Policy.

16. Related policies and monitoring

This policy should be read alongside our Safeguarding and Child Protection Policy, Behaviour Regulation Policy, Anti-bullying Policy, Staff Code of Conduct, Acceptable Use Policies, Mobile Phone Policy, Data Protection Policy, Remote Learning Policy, Whistleblowing Policy and PSHE and Relationships and Health Education Policy.

The DSLs and online safety lead monitor online safety incidents on CPOMS and report trends to the Headteacher and governors. This policy is reviewed every year, and sooner if guidance changes or following a serious incident.