Richard Cloudesley School

Online Safeguarding Policy

Updated: March 2026

Ratified by governors on: 6 March 2026

For review: March 2027

This policy is based on the following:

1. Keeping Children Safe in Education (KCSIE)
   - The statutory document for safeguarding in schools.
   - Includes mandatory expectations for online safety, filtering & monitoring, staff conduct, reporting, AI considerations and child protection.
   - Must be referenced in any online safety policy.

2. Working Together to Safeguard Children (2023, 2025 update)
   - Sets out multi-agency responsibilities.
   - Includes expectations around digital safeguarding, early help, and information-sharing.

3. DfE: Filtering and Monitoring Standards (2023)
   - The legally required national standards for IT filtering and monitoring in schools.
   - *Every* online safety policy must explain how the school meets these.

4. DfE: Teaching Online Safety in Schools (2019)
   - Provides guidance on curriculum expectations, the 4 Cs (Content, Contact, Conduct, Commerce), and age-appropriate education.

5. DfE: Generative Artificial Intelligence in Education (2024)
   - National guidance on safe, ethical and responsible use of AI in schools.
   - Directly informs your AI principles (transparency, fairness, accountability, contestability).

6. UK GDPR & Data Protection Act 2018
   - Defines lawful processing, data minimisation, retention, privacy, subject access, and data security requirements—including in the use of AI and digital platforms.

7. Education (Pupil Information) Regulations (2005)
   - Defines how pupil data must be stored, transferred and retained.

8. Prevent Duty Guidance (relevant to online radicalisation)
   - Sets expectations for mitigating online extremist content risk.

9. Guidance for Safer Working Practice for Adults Working with Children (2022 update)
   - Covers staff conduct online, communication boundaries, video calling, messaging, and social media expectations.

1. Statement of Policy & Purpose

This policy sets out how Richard Cloudesley School ensures the safe, ethical and effective use of digital technologies including cloud platforms (e.g. Microsoft Teams), email, mobile and smart devices, multimedia, and Artificial Intelligence (AI). It integrates previous Online Safety and Acceptable Use guidance into one coherent framework.

2. Scope

Applies to all pupils, staff, governors, contractors, visitors and volunteers, and to all school systems and devices used on-site or off-site for school purposes.

3. Definitions

Online risks are categorised as:

- Content (what pupils see)
- Contact (who they interact with)
- Conduct (how they behave)
- Commerce (financial risk, scams).

AI refers to systems that generate content or insights and must be used with transparency, safety and human oversight.

4. Roles & Responsibilities

Governing Body: provides strategic oversight and approves this policy.

Headteacher/SLT: treat online safety as a whole-school safeguarding responsibility and ensure resources and training.

DSL & OSL: lead digital safeguarding practice, maintain incident logs, liaise with agencies.

Technician: ensure technical controls, filtering/monitoring and data protection compliance.

Staff: model positive use, follow Acceptable Use and report concerns.

Pupils: follow the pupil agreement and report concerns. Parents/Carers: support safe use at home and comply with consent/photography rules.

Contractors/Visitors: comply with this policy while on site.

5. Acceptable Use – Staff

Staff must:

- maintain the highest standards of personal online behaviour. This includes ensuring that personal social media accounts, online profiles and digital communications do not bring the school into disrepute or risk exposing pupils or families to inappropriate content.

- not post images, videos or comments about pupils, families, colleagues or school matters on personal platforms.

- not engage in online communication, groups or forums with pupils, nor accept or initiate friend or follow requests from pupils or former pupils.

- Staff must manage their own digital footprint responsibly and uphold professional boundaries at all times.

- not view, upload or download inappropriate content. Vet online material before using with pupils.

- not share personal phone numbers or personal accounts with pupils or families.

- respect privacy of others' files and maintain strong passwords.

- publish pupil images only with parental consent and never match names to photos.

- log off when finished using devices or accounts.

6. Acceptable Use – Pupils

Pupils must follow these rules whenever they use school devices, online systems, or the internet:

Using Devices Safely

- Use school devices carefully and handle equipment responsibly.
- Keep devices clean, secure and follow any instructions given by staff.
- Tell an adult immediately if a device is damaged, not working properly or shows something unexpected.

Passwords & Personal Information

- Keep your passwords private — never share them with friends or anyone online.
- Use strong passwords and change them if an adult tells you to.
- Do not share personal information such as your full name, address, phone number, school route or details about your family.

Safe Online Behaviour

- Be kind and respectful when using any online platform.
- Think before you click: do not open messages, links or pop-ups that seem strange or upsetting.
- Report anything that worries you straight away to a trusted adult.

Respecting Others

- Respect other people's work, files and privacy.
- Do not edit, delete or look at anyone else's work unless a member of staff tells you to.
- Always ask before taking photos of others, even your friends.

Photos, Videos & Recording

- Do not take or share photos, videos or recordings on personal devices while at school.
- Only use school devices for photos/videos if a member of staff has given permission.
- Never upload or share photos or videos of others online.

Using the Internet & Apps

- Use only school-approved websites, apps and tools.
- Stick to the tasks your teacher has set and do not try to access blocked or unsuitable sites.
- Do not attempt to bypass school filters, change settings or use someone else's login.

If Something Goes Wrong

- Tell an adult straight away if:
    - You see something upsetting, scary or inappropriate
    - Someone online is unkind or asks you for personal information
    - A device stops working properly
- You will *never* be in trouble for reporting something that worries or confuses you.

7. Digital Communication (Email & Microsoft Teams)

Staff should only use Teams messages and email for professional communication during and only during working hours.

When messaging parents or posting on the Teams community, teaching assistants should check content of messages home with the class teacher. All staff should remember that Teams messages should not contain any potentially sensitive informative or personal data.

All online communication must be concise, use clear subjects, avoid large attachments, and should never unnecessarily disclose personal information of pupils, staff or governors. Personal information should be sent using secure email.

Emails from parents and Teams messages received during the school day may not be read until the end of the school day. For time sensitive matters requiring immediate attention, parents should contact by phone.

Emails

- Our policy is not to send emails outside of working hours. If staff need to compose an email outside of working hours, they are asked to use the scheduling feature or save it as a draft.
- We strongly advise staff to avoid checking emails outside of your working hours.
- No-one should mention anyone in an email unless they would be comfortable with them being copied in, as everyone have the right to read any email in which they are mentioned and may request to see it.
- We should never use 'Bcc' to blind copy people into an email.

Microsoft Teams Messages

- All staff are asked to set their Teams 'quiet times' to reflect your working hours.
- We encourage strongly advise all staff not to send or reply to Teams messages outside of working hours. If they need to wrote messages outside of working house they should use message scheduling.
- Staff should set their Teams / Office to 'busy' they are unable to check messages, for example in a meeting or teaching.

Staff Low-Level Concerns

If staff have concerns about colleagues, they must use the low-level concern form, and not include these concerns in Teams messages or emails to leaders.

8. Remote Learning & Live Video

Staff must use only school-approved devices and school accounts when making video calls with pupils. When a phone call is required, staff must ensure their caller ID is withheld to protect personal contact details. One-to-one video calls should be avoided wherever possible; they may only take place when explicitly authorised by a senior leader or the DSL/OSL, and clear justification must be recorded. Group calls are the preferred format as they provide increased transparency and safeguarding protection.

All staff must ensure they present themselves professionally during any video call. This includes wearing appropriate clothing, choosing a neutral or blurred background, and ensuring no

confidential or inappropriate material is visible. Calls must take place in an appropriate environment - never in bedrooms or private household spaces where boundaries could become blurred.

Video calls with pupils must only occur during the school day and within agreed working hours. Staff must not initiate or respond to calls outside these times. Before starting any call, staff must check that at least one additional adult is present on the pupil's side where appropriate, or ask who is in the room.

Staff should end the session immediately if they feel uncomfortable, unsure about supervision, or concerned about what they see or hear, and must report this to the DSL/OSL without delay.

Record-keeping expectations must be followed: the purpose of the call, attendees and any issues that arise must be noted. No part of the call may be recorded unless formally approved in advance and communicated to all participants.

9. Photography & Video

No photographs of pupils on personal devices. No photography in personal care areas. Publish media only with parental consent and never match pupil names to images.

10. Mobile & Smart Devices, including watches

Staff use of personal mobile phones and smart devices

Staff personal devices may access Teams for school communication where permitted, with passcode protection and no local storage of pupil data.

The school will set expectations for pupil and visitor device use on site, including camera restrictions and supervision.

Personal notifications should be switched off on all devices, including smart watches.

Work Phones

Some staff members, including IT staff and members of the leadership team, are issued with work phones to support safe, professional and appropriate school communication.

Pupil use of mobile phones and smart devices

Pupils are expected to follow the school's rules regarding the use of mobile phones and digital devices. Mobile phones should be switched off and kept out of sight during the school day unless permission has been given for educational purposes. The school will not tolerate cyberbullying or inappropriate online behaviour, whether it occurs on or off school premises. Incidents will be dealt with in line with the school's anti-bullying and safeguarding policies.

11. Emerging Technologies

The school recognises that new and emerging technologies, such as AI-enabled apps, smart pins, glasses and other wearables, connected toys and other automated systems, may introduce new risks.

The school will review and assess new technologies before adoption to ensure they are safe, appropriate and compliant with data protection, safeguarding and ethical standards.

12. User Accounts, Passwords & Network Access

To protect the security of the school network and the personal data it contains, all pupils, staff, governors, contractors and visitors must adhere to the following requirements:

- **Everyone must only use their own assigned login credentials** when accessing any school device, system, platform or network service (e.g. Microsoft 365, Teams, email, Arbour, Access, CPOMS).
- **Sharing passwords or logging in for someone else is strictly prohibited.**
- Staff must never use pupil accounts, and pupils must never use staff accounts. Pupils must only use their own accounts.
- Users must **keep passwords private**, secure, and not written down or stored in an unsecured location.
- Users must **log out of devices and systems** when they are not in active use to prevent unauthorised access.
- If a password is compromised or suspected to be compromised, users must **report it immediately** to the technician/OSL and change it without delay.
- The school may audit login activity where required for safeguarding, security or data-protection purposes.

13. Password Security & Authentication

To protect the school network and personal data, all users must follow the school's password and authentication standards. Passwords must be strong, unique, not shared with anyone, and changed immediately if compromise is suspected. Access to sensitive systems may require multi-factor authentication. The school may enforce password-reset cycles, security checks and monitoring to ensure compliance with DfE Cyber Security Standards.

14. Online Sexual Harassment & Harmful Sexual Behaviour

The school recognises that online sexual harassment and harmful sexual behaviour can occur between pupils and may include the sending or sharing of sexualised images ("nudes" or "semi-nudes"), unwanted sexualised comments, coercion or pressure online, and the non-consensual distribution of images. These behaviours are treated as safeguarding concerns. Any such incident must be reported immediately to the DSL/OSL and will be managed in line with national guidance, including referral to external agencies where appropriate.

15. Online Bullying & Behaviour Expectations

All online conduct between pupils is subject to the same expectations outlined in the school's Behaviour Policy. Cyberbullying, harassment or online intimidation will be treated with the same seriousness as offline behaviour. Pupils will be supported to act responsibly online, understand the impact of their actions, and report online bullying promptly.

16. Digital Wellbeing

The school promotes healthy use of digital technologies and supports pupils to understand the impact of screen time, online pressure and the emotional effects of digital interactions. Staff encourage balance, positive online habits and regular breaks from devices. Pupils are taught

strategies to manage online stress, limit exposure to harmful content, and seek help when feeling overwhelmed.

17. Filtering & Monitoring

The school operates age-appropriate internet filtering and device monitoring. The DSL retains strategic oversight, supported by the technician. Staff receive induction on the system, how to escalate concerns, and how over-blocking is avoided to ensure curriculum access. Alerts and logs are reviewed routinely and acted on.

18. Curriculum – Teaching Online Safety

Online safety is delivered through a planned curriculum (e.g. PSHE and Computing), reinforced in assemblies and tutor time, and supported by external agencies where appropriate. Teaching includes digital citizenship, recognising risk, respectful online behaviour, critical evaluation of content, and understanding consent and privacy.

Pupils are taught to recognise online financial risks, including scams, phishing attempts, subscription traps, fraudulent adverts, and in-app purchases. The school's filtering and monitoring systems aim to reduce commercial exploitation risk, while the curriculum supports pupils in developing critical awareness when engaging with commercial content online.

19. Artificial Intelligence (AI) – Principles & Practice

AI is used to reduce workload and enhance learning where appropriate, in line with principles of safety, transparency, fairness, accountability and contestability.

Staff remain responsible for decisions and must review AI-generated material for accuracy and bias.

No personal data is to be entered into AI tools without a lawful basis.

Staff and pupils must label AI-assisted work where appropriate.

Under the Regulation of Investigatory Powers
Act 2000 (RIPA), individuals may legally record conversations or phone calls they participate in f or personal use without obtaining consent from other parties. If AI transcripts are intended to be used beyond personal use, then all parties must be informed that the transcript is taking place. Transcripts and associated AI summaries must be confirmed for accuracy before being shared, as we would do for any meeting minutes.

20. Data Protection & Retention

Only collect and share personal data when necessary.

Transfer information that forms part of a record (e.g. safeguarding, MIS) into the correct system; do not use Teams or email as long-term storage.

Follow retention schedules and securely delete data when no longer required.

21. Incident Reporting & Response

Report online safety concerns immediately to the OSL/DSL. All incidents are logged, investigated and, where necessary, escalated to external agencies. The OSL and technician meet regularly to review incident data, blocked sites and trends, and to adjust controls and education accordingly.

In addition to reporting concerns internally, pupils and parents may also access external reporting and support routes. This includes the CEOP Safety Centre for reporting online grooming or exploitation concerns, child protection services, and in emergencies, the police. The school will signpost families to recognised national helplines and online safety organisations for additional guidance and support.

21. Training & Awareness

All staff receive online safety and data protection induction and regular refresher training. Records of attendance are maintained. Targeted training is provided where risks or roles require it.

22. Technical & Network Security

The technician maintains a secure infrastructure, implements updates and access controls, and supports monitoring. Regular reviews and audits are undertaken with SLT/OSL to confirm effectiveness and address emerging risks.

23. Partnerships with Parents/Carers

The school shares guidance and updates with families, promotes safe use at home, and sets clear expectations for parent use of school systems. Parental consent is managed for imagery and online services where required.

24. Governance Oversight

Termly reports on online safety (incidents, training, filtering/monitoring, curriculum) are provided to governors. Governors scrutinise impact and challenge leaders where improvements are needed.

25. Communication & Implementation

This policy is communicated to staff during induction and published for the school community.

Key expectations are displayed in staff and pupil areas.

26. Monitoring, Review & Audit

SLT, DSL and OSL review incidents, training and system data at least termly. An annual audit informs updates to this policy and related procedures.

27. Related Policies & Documents

To be read alongside:

- Safeguarding & Child Protection

- Behaviour & Anti-Bullying; Data Protection
- Freedom of Information
- Health & Safety
- Remote Learning
- Data Retention
- Equality
- Photography/Media Consent
- Staff Code of Conduct.

Pupil-Friendly Summary: Using Technology Safely

- Keep your passwords private and your device safe.
- If something online worries or upsets you, tell an adult straight away.
- Be kind and respectful when you are online.
- Never share personal information (like your full name, address or school route).
- Only use websites and apps your teacher has approved.
- Do not take photos or videos without permission. Never post pictures of others without checking with an adult.
- If you are not sure, ask an adult for help.