Online Safety Policy

Date established by governing body Autumn Term 2026 **Date for full implementation** Immediately **Date for review** Autumn Term 2027

Policy Statement

Cleaswell Hill School is committed to safeguarding and promoting the welfare of all pupils and recognises that online safety is an essential part of this responsibility. The school believes that digital technologies offer significant opportunities to support learning, communication, independence, preparation for adulthood and participation in modern society. However, we also recognise that technology can expose children and young people to risks, particularly children with Special Educational Needs and Disabilities (SEND), who may experience increased vulnerability online.

Online safety forms an integral part of the school's safeguarding culture and is embedded within leadership, governance, curriculum delivery, behaviour systems, staff training, safeguarding procedures and communication with families.

The school adopts a child-centred approach and recognises that safeguarding incidents and concerns can occur both online and offline. Online concerns will therefore be managed in line with the school's Child Protection and Safeguarding Policy and relevant statutory guidance.

Aims

This policy aims to:

- Protect pupils from online harm.
- Promote safe, responsible and respectful use of technology.
- Ensure compliance with statutory safeguarding requirements.
- Support pupils to develop digital resilience and independence.
- Ensure staff understand their safeguarding responsibilities relating to online safety.

- Establish clear procedures for preventing, identifying, reporting and responding to online safety concerns.
- Ensure effective governance and leadership oversight.
- Promote a whole-school culture where online safety is everyone's responsibility.

Legislative and Statutory Framework

This policy should be read alongside:

- Keeping Children Safe in Education 2026 (KCSIE)
- Working Together to Safeguard Children
- Relationships Education, Relationships and Sex Education (RSE) and Health Education Statutory Guidance (effective September 2026)
- The Prevent Duty Guidance
- Education for a Connected World Framework
- DfE Filtering and Monitoring Standards
- UK GDPR
- Data Protection Act 2018
- Behaviour is Communication Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- ICT and Acceptable Use Policy
- Mobile Phone and Personal Devices Policy
- Use of AI (Artificial Intelligence) Policy
- Safeguarding and Child Protection Policy

The governing body recognises that online safety is a safeguarding issue and must be managed through a whole-school and whole-setting approach.

Online Safety Policy

Roles and Responsibilities

Governing Body

The governing body will:

- Ensure appropriate safeguarding arrangements for online safety.
- Ensure appropriate filtering and monitoring systems are in place.
- Receive regular online safety reports.
- Review online safety risks and emerging technologies.
- Oversee annual evaluation of filtering and monitoring arrangements.
- Ensure adequate resources and staff training are available.

KCSIE requires governance oversight of online safety and filtering and monitoring arrangements.

Headteacher

The Headteacher will:

- Ensure implementation of this policy.
- Promote a strong culture of safeguarding.
- Ensure staff training is provided.
- Support effective safeguarding responses to online incidents.
- Ensure online safety remains a standing safeguarding priority.

Designated Safeguarding Lead (DSL)

The DSL with support from the CEOP Ambassador:

- Lead on online safeguarding.
- Manage online safety concerns.
- Monitor safeguarding trends.
- Liaise with external agencies where necessary.
- Ensure safeguarding records are maintained.

- Work closely with technical staff on filtering and monitoring arrangements.
- Provide advice and support to staff, pupils and families.

Staff

All staff will:

- Understand that online safety is a safeguarding responsibility.
- Read and understand KCSIE Part One.
- Report concerns immediately to the DSL.
- Model safe and professional technology use.
- Deliver safeguarding messages through the curriculum where appropriate.

Understanding Online Risks

The school recognises the four areas of online risk:

Content

Exposure to:

- Extremist material
- Harmful content
- Misinformation and disinformation
- Self-harm content
- Pornographic content
- AI-generated harmful content

Contact

Risks relating to:

- Grooming
- Sexual exploitation
- Criminal exploitation
- Radicalisation
- Coercion
- Manipulation

Conduct

Including:

- Cyberbullying
- Harassment
- Child-on-child abuse
- Hate incidents
- Image sharing
- Image based abuse
- Online abuse
- Prejudicial and discriminatory bullying

Commerce

Including:

- Scams
- Fraud
- Gambling
- Financial exploitation
- Inappropriate commercial content

These risks may affect SEND pupils differently and may require additional support and protective measures.

Online Safety Policy

Artificial Intelligence and Emerging Technologies

The school recognises the increasing safeguarding risks associated with:

- Generative AI
- Deepfakes
- Manipulated images and videos
- AI chatbots
- Nudification applications
- Sextortion
- Image-based abuse
- AI-generated sexual content

Pupils will be taught age and developmentally appropriate AI literacy skills through Computing, PSHE and RSHE education.

Staff will receive training to identify and respond to emerging risks associated with artificial intelligence and evolving digital technologies.

The school will assess safeguarding implications before introducing new digital technologies or AI tools.

The 2026 guidance strengthens expectations around awareness of AI-generated harms and online safeguarding arrangements.

Online Safety Education

Online safety education is embedded throughout:

- Computing
- PSHE
- RSHE
- Safeguarding curriculum
- Personal Development
- Preparation for Adulthood pathways

Pupils will learn about:

- Healthy online relationships
- Consent
- Privacy
- Personal boundaries
- Password security
- Digital footprints
- Reporting concerns
- Image sharing
- Fake news and misinformation
- Online exploitation
- Cyberbullying
- AI awareness
- Online reputation
- Respectful communication

Teaching will be differentiated to meet the needs of pupils with SEND and delivered at an appropriate developmental level.

The revised RSE and Health Education guidance places increased emphasis on safety, healthy relationships, consent, personal boundaries and online safety.

Remote learning arrangements should be read alongside the Department for Education guidance on Providing remote education: guidance for schools and Safeguarding and remote education, Keeping Children Safe in Education, the school's Safeguarding and Child Protection Policy, ICT and Acceptable Use Policy, Data Protection Policy, Staff Code of Conduct and relevant SEND and attendance procedures.

Policy and statutory reference

Because Cleaswell Hill School is a specialist setting, remote provision will be adapted to the pupil's communication, cognition and learning, sensory, physical, medical and social-emotional needs. Staff will consider accessibility features, alternative methods of communication and recording, assistive technology, parental support and the practical limitations of delivering specialist or therapeutic provision remotely. Where remote

education cannot reasonably replicate required specialist provision, leaders will consider alternative arrangements with the family and, where relevant, the local authority and other professionals.

Remote Learning and SEND

Remote learning activity conducted through school systems may be monitored, logged and reviewed to support safeguarding, security and compliance with school policies. Filtering and monitoring arrangements will apply to school-managed systems and devices in accordance with the school's filtering and monitoring arrangements. Users must follow the ICT and Acceptable Use Policy, Data Protection Policy and Online Safety Policy when accessing remote learning resources. Filtering and monitoring will not replace active supervision, appropriate teaching, professional curiosity or safeguarding procedures.

Monitoring and Security of Remote Learning

Pupils, parents/carers and staff should report concerns arising from remote learning or online communication using the school's normal safeguarding and reporting procedures. Concerns may include inappropriate content, online bullying, unauthorised contact, unsafe online behaviour, security or privacy concerns, or technical issues that may affect safety. The school will investigate concerns proportionately and take appropriate action in accordance with safeguarding, behaviour and data protection procedures.

Reporting Online Safety Concerns

All safeguarding responsibilities continue to apply during periods of remote learning. If a member of staff becomes aware of a welfare concern, safeguarding concern, online abuse or exploitation, inappropriate online behaviour, or a disclosure made through an online platform, they must follow the school's safeguarding procedures immediately and report the concern to the Designated Safeguarding Lead (DSL) or Deputy DSL without delay. Staff must not undertake their own investigation.

Safeguarding During Remote Learning

Staff must maintain the same professional standards online as they would in face-to-face interactions. This includes maintaining appropriate professional boundaries; using only school-approved accounts and systems; ensuring communications are transparent, professional and auditable; and avoiding communication that could be interpreted as personal, private or inappropriate. Any concern relating to professional conduct online must be reported in accordance with the school's safeguarding, staff conduct and whistleblowing procedures.

Professional Conduct and Boundaries

Online Safety Policy

The school does not require pupils to use cameras as part of its remote learning provision. Staff must not require pupils to activate cameras or share video from their home environment unless specific arrangements have been approved by school leaders and parents/carers have been informed. Where video is used, staff should consider privacy, safeguarding, accessibility and the individual circumstances of the pupil and family.

Camera Use

The school's remote learning model does not routinely include live teaching sessions, video calls or camera-based learning activities. Where exceptional circumstances require a live online meeting, prior approval must be obtained from a member of the Senior Leadership Team, a school-approved platform must be used, safeguarding and professional standards must be followed, and parents/carers will be informed where appropriate. Any live session must use appropriate privacy and security settings and clear expectations for participation.

Live Teaching and Video Communication

Staff may communicate with pupils through written comments, feedback tools, assignment functions and messaging features within approved educational platforms. All communication must be professional and educational in nature; relate directly to teaching, learning, wellbeing or safeguarding; take place through school-approved platforms; and, wherever possible, be conducted during reasonable working hours. Communications must be capable of appropriate school oversight for safeguarding and professional accountability. Staff must not communicate with pupils using personal email addresses, personal social media accounts, personal telephone numbers or private messaging applications.

Communication and Feedback

Remote learning and home learning activities will only be delivered through school-approved platforms and systems. The school currently uses Microsoft Teams and other approved educational applications to provide learning materials, assignments, feedback and communication. Staff, pupils and families must only use approved school systems when accessing remote learning activities. Platforms must be appropriately secured, kept up to date and used in accordance with the school's ICT, Acceptable Use, Data Protection and Online Safety requirements.

Approved Platforms

The school will ensure that remote learning provision is safe, accessible and consistent with safeguarding, data protection, online safety and professional conduct requirements. Remote education arrangements will be reviewed where a pupil's

circumstances change or where the provision is not meeting the intended educational or safeguarding purpose.

Remote learning is not used as a routine method of education at Cleaswell Hill School. It may be offered where a pupil is unable to attend school for a limited or exceptional period but is well enough to continue learning, including because of medical needs, individual circumstances, or other exceptional reasons. It may also support home learning through approved digital platforms. Remote education will be used only where appropriate to the pupil's circumstances and will not replace provision that the school or local authority is required to secure under an EHC plan or the Equality Act 2010. The school will consider reasonable adjustments, accessibility and the pupil's individual SEND needs when remote provision is planned.

Remote Learning and Online Education Provision

Filtering and Monitoring

The school maintains filtering and monitoring systems that:

- Protect pupils from harmful content.
- Support identification of safeguarding concerns.
- Meet DfE standards.
- Include consideration of AI-generated content and evolving digital risks.
- Are reviewed at least annually.

The school will ensure:

- Leadership understand filtering and monitoring systems.
- DSLs understand safeguarding alerts generated through monitoring.
- Technical staff and safeguarding staff work collaboratively.
- Safeguarding concerns are escalated promptly.

Filtering and monitoring systems form part of the school's wider safeguarding arrangements and cannot replace active supervision, education and professional curiosity.

Mobile Devices and Personal Technology

The use of personal devices by staff, volunteers and visitors must comply with:

- Staff Code of Conduct
- Data Protection requirements
- Safeguarding procedure
- Mobile phone and personal devices policy

Unauthorised recording or photography is prohibited.

Responding to Online Safety Concerns

All concerns will be treated as safeguarding concerns.

Examples include:

- Online grooming.
- Sextortion.
- Sharing nude or semi-nude images.
- Deepfake abuse.
- Cyberbullying.
- Online harassment.
- Radicalisation concerns.
- Exploitation.
- Harmful online content.
-

Staff must:

1. Listen and reassure.
2. Preserve evidence where appropriate.
3. Avoid investigating independently.
4. Record concerns promptly.
5. Report concerns to the DSL immediately.

Online Safety Policy

Child-on-Child Abuse Online

The school recognises that online child-on-child abuse can include:

- Sexual harassment
- Sexual violence
- Image-based abuse
- Sharing of nude images
- Deepfake sexual imagery
- Cyberbullying
- Coercive behaviour
- Abuse through gaming and social media platforms

All incidents will be managed in line with the Safeguarding and Child Protection Policy.

Working with Parents and Carers

The school will:

- Share online safety information with families.
- Promote parental awareness of online risks.
- Offer guidance regarding gaming, social media and technology use.
- Encourage parents to report concerns.

Strong partnerships with parents are recognised as an essential component of effective safeguarding.

Staff Training

All staff will receive:

- Annual safeguarding updates.
- Online safety training.
- Emerging technology awareness training.
- Filtering and monitoring awareness.

- Training regarding vulnerabilities associated with SEND.
- AI and online harm awareness updates.

Policy Monitoring and Review

This policy will be reviewed:

- Annually.
- Following significant safeguarding incidents.
- Following changes in legislation or national guidance.
- Following Ofsted recommendations.

Author: Helen McIntyre/ Emma Dunn
Headteacher: Mike Jackson
Chair of Governors: Tim Chrisp
Date: Autumn 2026