

Policy written by: Headteacher / Designated Safeguarding Lead (DSL)

Approved by: Governing Body – September 2026

Review Date: Annually

Linked Policies: Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct, Data Protection Policy, Acceptable Use Agreements

1. Statement of Intent

Clover Hill Primary School recognises that technology plays an important role in the lives of children and young people. We are committed to ensuring that all members of the school community are able to use digital technologies safely, responsibly and positively.

This policy supports the school's commitment to safeguarding and promoting the welfare of children and should be read alongside the school's Safeguarding and Child Protection Policy.

The school acknowledges its duties under **Keeping Children Safe in Education (KCSIE) 2026**, which states that online safety is an integral part of safeguarding and requires schools to have effective arrangements in place to protect children from online harm. KCSIE 2026 emphasises the importance of educating children about online safety, maintaining effective filtering and monitoring systems, and addressing emerging risks, including those associated with artificial intelligence (AI), deepfake imagery, online exploitation and harmful online content.

2. Aims

The aims of this policy are to:

- Safeguard pupils whilst they access and use digital technologies.
- Promote safe and responsible online behaviour.
- Ensure staff understand their roles and responsibilities regarding online safety.
- Educate pupils about online risks and how to seek support.
- Support parents and carers in keeping children safe online.
- Ensure effective filtering and monitoring arrangements are in place.
- Respond effectively to any online safety concerns or incidents.
- Establish clear expectations for the acceptable use of technology.

3. Legislative and Statutory Framework

This policy has been developed in accordance with:

- Keeping Children Safe in Education (KCSIE) 2026.
- The Education Act 2002.
- Data Protection Act 2018 and UK GDPR.
- Working Together to Safeguard Children.

- Teaching Online Safety in Schools (DfE).
 - National Curriculum for Computing (Key Stages 1 and 2).
-

4. Roles and Responsibilities

The Governing Body will:

- Ensure that online safety is embedded within the school's safeguarding arrangements.
- Oversee the effectiveness of online safety provision.
- Ensure appropriate filtering and monitoring systems are in place and reviewed annually, as required by KCSIE 2026.
- Receive regular safeguarding and online safety updates from school leaders.

The Headteacher will:

- Ensure implementation of this policy.
- Promote a whole-school culture of online safety.
- Ensure staff receive regular online safety training.

The DSL will:

- Lead on online safety as part of safeguarding.
- Manage concerns relating to online abuse, exploitation, cyberbullying or harmful content.
- Liaise with external agencies where necessary.
- Ensure staff understand reporting procedures.
- Monitor emerging safeguarding risks.

All staff will:

- Model safe and professional online behaviour.
- Deliver online safety education where appropriate.
- Report concerns immediately in line with safeguarding procedures.
- Understand the school's filtering and monitoring systems in accordance with KCSIE 2026.

Pupils are expected to:

- Use technology safely, respectfully and responsibly.
- Follow the school's acceptable use expectations.
- Report anything online that worries or upsets them.
- Respect the rights and privacy of others.

Parents and carers are encouraged to:

- Support the school's online safety messages.
 - Monitor their child's use of technology at home.
 - Report concerns to school where appropriate.
 - Engage with online safety information shared by the school.
-

5. Online Safety Education

The school recognises that teaching online safety is essential in helping pupils to become responsible digital citizens.

Key Stage 1

In line with the National Curriculum for Computing, pupils will be taught to:

- Use technology safely and respectfully.
- Keep personal information private.
- Recognise when content or contact online makes them feel uncomfortable.
- Know who to speak to when they have concerns.

Key Stage 2

In line with the National Curriculum for Computing, pupils will be taught to:

- Use technology safely, respectfully and responsibly.
- Understand acceptable and unacceptable online behaviour.
- Recognise risks associated with online communication.
- Protect personal information and passwords.
- Evaluate online content critically.
- Understand how to report concerns and seek help.

Wider Curriculum

Online safety is taught through:

- Computing
- RSHE
- PSHE
- Assemblies
- Safeguarding lessons
- Awareness campaigns and themed events

Teaching reflects current risks including:

- Cyberbullying
- Online exploitation
- Inappropriate content
- Misinformation and disinformation
- Gaming risks
- Social media
- Privacy and personal information
- AI-generated content, deepfakes and manipulated images
- Healthy online relationships

6. Managing Online Risks

The school recognises that online risks can broadly be categorised into:

- **Content:** exposure to harmful, illegal or inappropriate material.
- **Contact:** harmful interaction with others online.
- **Conduct:** behaviour online that may cause harm.
- **Commerce:** risks linked to gambling, scams or financial exploitation.

The school will take proactive measures to reduce these risks through education, supervision and technical controls.

7. Filtering and Monitoring

The school maintains appropriate filtering and monitoring systems to safeguard pupils when using school technology.

These arrangements:

- Block access to inappropriate material.
- Help identify safeguarding concerns.
- Are reviewed regularly and formally evaluated at least annually.
- Support wider safeguarding arrangements rather than being viewed solely as technical measures.

Staff receive information about the school's filtering and monitoring arrangements and their safeguarding responsibilities.

8. Use of Artificial Intelligence (AI)

The school recognises the increasing use of artificial intelligence technologies and associated safeguarding risks.

Pupils will be taught:

- How AI tools work in an age-appropriate manner.
- To critically evaluate content generated by AI.
- About the risks associated with deepfakes, manipulated images and misinformation.
- To report concerns where AI technologies may be used to harm, deceive or exploit others.

Any use of AI within school will be carefully supervised and aligned with safeguarding, privacy and educational requirements.

9. Cyberbullying

Cyberbullying will not be tolerated.

Incidents may include:

- Offensive messages.
- Sharing images without consent.
- Exclusion from online groups.
- Harassment or intimidation via digital platforms.

Any incidents will be investigated and addressed in accordance with the school's Behaviour Policy and Anti-Bullying Policy.

10. Responding to Online Safety Concerns

All online safety concerns will be treated as safeguarding concerns where appropriate.

Staff must:

1. Reassure the child.
2. Record the concern promptly on CPOMS.
3. Inform the DSL immediately.
4. Preserve evidence where possible.
5. Avoid investigating independently.

The DSL will assess risk and take appropriate action, including referral to external agencies where necessary.

11. Staff Training

All staff will receive:

- Annual safeguarding training.
- Regular updates regarding online safety.
- Information about new and emerging online risks.
- Training relating to filtering and monitoring arrangements (DSLs)

New staff will receive online safety information as part of induction.

12. Working with Parents and Carers

Clover Hill values partnership working with parents and carers and will:

- Share online safety guidance regularly.
 - Provide updates about emerging risks.
 - Signpost families to trusted sources of advice and support.
 - Encourage consistent messages between home and school.
-

13. Monitoring and Review

This policy will be reviewed annually or sooner if:

- Legislation changes.
- New safeguarding guidance is issued.
- Emerging technologies create new risks.
- A significant online safety incident occurs.

The Governing Body will receive updates regarding the effectiveness of the school's online safety arrangements and compliance with KCSIE requirements.