

Hamsey Green Primary School

Online Safety Policy



Policy Reviewed: July 2026
Next Review Date: July 2027
Reviewer: Steve Brown (Computing Lead)

1. Purpose and scope

Hamsey Green Primary School recognises that safeguarding pupils online is an integral part of safeguarding and is inseparable from the school's wider culture, curriculum, behaviour expectations, data protection, cyber security and child protection arrangements. This policy applies to pupils, staff, governors, volunteers, contractors and visitors, and to school-provided technology whether used on site or remotely.

The policy covers school networks and accounts, internet access, filtering and monitoring, email and messaging, social media, mobile and wearable devices, online learning, images and video, gaming and immersive environments, generative artificial intelligence (AI), data protection, cyber security and online incidents that affect the safety or wellbeing of members of the school community.

2. Core principles

Online safety is a safeguarding responsibility, not solely an IT responsibility.

The school will protect pupils through education, appropriate technical controls, clear reporting routes and proportionate responses to incidents.

Pupils will be taught to recognise risk, make safe choices, seek help and behave respectfully online.

A child-centred and contextual approach will be used, with additional consideration for pupils who may be more vulnerable online, including pupils with SEND.

Technology, including AI, will be used where it adds educational value and can be used safely, lawfully, ethically and with appropriate human oversight.

3. The four areas of online risk

The school uses the four-area framework of content, contact, conduct and commerce when considering online safety risks.

Content

Pornographic, violent, extremist, hateful, discriminatory, self-harm, suicide, eating-disorder or other harmful content.

Misinformation, disinformation, conspiracy material, scams, manipulated media, synthetic media and AI-generated content that may appear authentic.

Age-inappropriate games, apps, videos, livestreams, algorithmically recommended content and advertising.

Contact

Grooming, sexual exploitation, coercion, radicalisation, unwanted contact, impersonation and contact from strangers.

Online bullying, harassment, abusive messaging and pressure to share images or personal information.

AI chatbots or companion-style systems that may encourage inappropriate disclosure, dependency, manipulation or unsafe advice.

Conduct

Cyberbullying, discriminatory abuse, harmful challenges, oversharing, poor digital citizenship and damage to digital reputation.

Sharing nude or semi-nude images, sexual harassment, non-consensual image sharing and AI-generated or manipulated sexual imagery.

Misuse of another person's identity, account, image, voice or work, including deepfakes and synthetic media.

Inappropriate use of generative AI for deception, bullying, plagiarism, fabrication or bypassing learning.

Commerce

Phishing, fraud, scams, identity theft, in-app purchasing, gambling-style mechanics, inappropriate advertising and financial exploitation.

Commercial collection or use of children's data, including profiling and persuasive design.

4. Roles and responsibilities

Governing Board

Ensures appropriate online safety arrangements, filtering and monitoring systems are in place and that responsibilities are clearly assigned.

Receives assurance that filtering and monitoring are reviewed at least annually and that identified risks, including generative AI risks, are addressed.

Ensures online safety is an interrelated theme across safeguarding, behaviour, curriculum, data protection and technology governance.

Headteacher and Safeguarding team

The Headteacher has overall responsibility for implementation. The DSL takes lead safeguarding responsibility for online safety and ensures online concerns are managed under child protection procedures.

The DSL and dDSLs understands the school's filtering and monitoring provision, receives relevant safeguarding information and ensures concerns are acted upon.

Concerns about staff conduct are referred to the Headteacher; concerns about the Headteacher are referred in accordance with the school's whistleblowing procedures which state that any concerns should be made to the Chair of Governors.

Online Safety / Computing Lead and IT support

Support curriculum delivery, staff awareness and safe use of technology.

Maintain effective technical controls and provide understandable reports to appropriate safeguarding and senior leaders.

Ensure changes to filtering, monitoring or access controls are authorised, documented and auditable.

All staff

Follow the staff code of conduct, acceptable use requirements, safeguarding procedures and data protection requirements.

Report online safety and safeguarding concerns promptly through the school's agreed recording system and to the DSL where required.

Use only approved school accounts and systems for professional communication with pupils and families. Check the suitability and safety of digital and AI tools before pupil use and follow school approval processes.

5. Filtering and monitoring

The school will maintain age-appropriate filtering and monitoring that reflects its safeguarding risk profile. Filtering is preventative and monitoring is reactive; neither replaces supervision, curriculum teaching or professional judgement.

Filtering will block illegal and inappropriate content without unreasonably restricting teaching and learning. Monitoring will support identification of potentially harmful activity and provide reports or alerts that can be understood and acted upon by trained staff.

Where practicable, users will be identifiable so concerns can be traced to an individual. Guest and shared access will be managed carefully.

The school will consider coverage on school devices used both on and off site and recognise that apps, mobile technologies and AI services may require controls beyond traditional web filtering.

Provision will be formally reviewed at least annually and following significant incidents, system changes or emerging risks. The review will include the school's pupil risk profile, SEND and vulnerability, remote access, mobile/app use and generative AI.

Filtering and monitoring staff will receive appropriate safeguarding training and have clear escalation routes to the DSL.

6. Artificial intelligence (AI)

Generative AI can create text, images, audio, video, code and other content. The school recognises potential benefits for teaching, accessibility, workload and administration, while also recognising safeguarding, accuracy, bias, privacy, intellectual property and developmental risks.

Approved use

Staff will use AI only where its use is consistent with school-approved systems, safeguarding expectations, data protection requirements and professional responsibilities.

AI outputs must be checked by a competent adult before being relied upon or shared with pupils. AI-generated information must not be assumed to be accurate, unbiased, current or age appropriate.

AI should support, not replace, professional judgement, teacher-pupil relationships, assessment of pupil need or safeguarding decision-making.

Pupil-facing AI use must be age appropriate, educationally justified, supervised as appropriate and consistent with the provider's terms, age requirements and school risk assessment.

Data and privacy

Staff and pupils must not enter personal, special category, confidential or safeguarding information into public or unapproved AI systems.

Before an AI product is adopted, the school will consider data processing, retention, training use, international transfers, security, age assurance, account requirements and whether a DPIA or other assessment is needed.

The school will consider the DfE's generative AI product safety standards when assessing AI products for educational use.

AI safeguarding risks

The school will address deepfakes, synthetic sexual imagery, impersonation, voice cloning, harmful generated content, scams, misinformation, manipulation and inappropriate chatbot interactions within safeguarding education and incident procedures.

AI-generated or AI-altered material used to bully, harass, sexualise, threaten, deceive or humiliate another person will be treated seriously under safeguarding and behaviour procedures, regardless of whether the material depicts a real event.

Staff must report suspected AI-related safeguarding concerns to the DSL. Staff should preserve relevant evidence without unnecessarily viewing, copying or redistributing illegal or harmful material.

AI literacy and learning

Pupils will learn that AI can produce convincing but false information and images and will be taught age-appropriate ways to question provenance, verify claims and recognise manipulation.

Pupils will be taught that AI-generated work does not remove responsibilities relating to honesty, authorship, copyright and respectful behaviour.

Teachers will make expectations about permitted AI assistance clear for learning activities. Pupil work and assessment should reflect the pupil's own knowledge and skills unless AI use is explicitly part of the task.

The school will teach pupils not to disclose personal information to AI tools and that chatbot responses are generated by systems, not trusted adults or friends.

7. Curriculum and pupil education

Online safety will be taught through Computing, Relationships and Health Education/PSHE and across the wider curriculum, with regular reinforcement through assemblies, class discussion and response to emerging issues.

Teaching will cover privacy, passwords, digital footprint, respectful communication, bullying, reporting, healthy technology use, online relationships, scams, copyright and age-appropriate sexual harassment and image-sharing risks.

Pupils will learn to evaluate online information, including misinformation, disinformation, hoaxes, manipulated media and AI-generated material.

Teaching will be adapted for age, developmental stage, SEND, communication needs and known vulnerabilities. A one-size-fits-all approach will not be assumed.

Pupils will know how to report something that worries, frightens, pressures or confuses them and will be reassured that reporting is the correct response.

8. Acceptable use and accounts

All staff must agree to the Staff Acceptable Use Agreement before accessing school systems. Pupil expectations will be taught and agreed in an age-appropriate form.

Passwords and authentication details must not be shared. Users must not access another person's files or account.

Only approved email, messaging, cloud and learning platforms may be used for school business.

Users must not deliberately bypass filtering, monitoring, security controls or restrictions.

Software, browser extensions, apps and AI services must not be installed or connected to school systems without appropriate approval.

9. Social media, messaging and online communication

Professional and private communication must remain separate. Staff must not use personal accounts to

communicate with pupils.

Staff must not discuss confidential matters relating to pupils, families or colleagues on personal social media.

School social media and publishing will use authorised accounts, appropriate permissions and editorial oversight.

Pupils will be taught about age restrictions, privacy settings, group chats, livestreaming, online reputation, location sharing, impersonation and reporting/blocking tools.

10. Mobile phones, smart devices and wearables

Pupil mobile phones brought to school will be managed under the school's agreed procedures and must not be used during the school day unless specifically authorised.

Staff and visitors must follow school expectations for secure storage and use of personal devices around pupils.

Images, audio or video of pupils must not be captured on personal devices unless expressly permitted under an approved school procedure.

Smart watches, wearable cameras, voice assistants and other connected devices will be subject to the same principles where they can record, communicate, locate or access online services.

11. Images, video and pupil work

The school will use images and video in accordance with its privacy notices, data protection arrangements and consent/other lawful basis requirements as applicable.

Personal contact details will not be published. School-managed publishing will be overseen by authorised staff.

Pupils will be taught that images can be copied, altered, AI-manipulated and redistributed, and that permission should be sought before sharing images of others.

12. Data protection and cyber security

Personal data will be handled in accordance with current data protection law, school policies and privacy notices.

The school will maintain appropriate access controls, updates, backups, malware protection, account management and cyber security arrangements.

Phishing, suspicious links, unexpected attachments, compromised accounts and data incidents must be reported promptly.

School data must not be transferred to personal accounts, unapproved cloud storage or unapproved AI

tools.

New technology and EdTech procurement will consider safeguarding, security, privacy, accessibility, contractual and data protection implications before deployment.

13. Responding to incidents

Online incidents will be considered through both safeguarding and behaviour lenses. The school will respond proportionately, prioritising the safety and welfare of the child.

Safeguarding concerns must be reported to the DSL and recorded through the school's safeguarding system in line with the Child Protection and Safeguarding Policy.

Where content may be illegal, staff must not investigate beyond what is necessary to safeguard the child and should follow DSL/police/local authority guidance.

Relevant evidence such as URLs, usernames, dates and contextual information may be recorded where safe and lawful; illegal images must not be copied or redistributed.

Incidents involving bullying, sexual harassment, nude or semi-nude images, extremist content, fraud, threats, impersonation, deepfakes or AI-generated abuse will be managed under the relevant safeguarding, behaviour and statutory procedures.

The school will consider whether filtering, monitoring, curriculum, risk assessments, staff training or parental communication need to change following an incident.

14. Parents, carers and the wider community

The policy and key expectations will be communicated through the school website, induction, newsletters and other appropriate channels.

Parents and carers will receive information and opportunities to develop understanding of current online risks, parental controls, social media, gaming, scams, image sharing and AI.

The school will encourage open conversations at home and will signpost reliable support where appropriate.

Visitors, contractors and community users of school technology must follow relevant acceptable use and safeguarding requirements.

15. Staff training

Online safety will form part of safeguarding induction and regular safeguarding updates.

Training will include filtering and monitoring responsibilities, emerging online harms, cyber security, data protection and safe use of generative AI.

Staff using AI will be expected to understand the risks of inaccurate output, bias, privacy breaches, intellectual property issues, safeguarding concerns and over-reliance.

16. Monitoring, review and linked policies

This policy will be reviewed at least annually. The school will also review it when there is a significant safeguarding incident, material change in technology or school systems, or relevant change in statutory guidance or law.

This policy should be read alongside the Child Protection and Safeguarding Policy, Staff Code of Conduct, Behaviour Policy, Anti-Bullying Policy, Data Protection Policy, Privacy Notices, Cyber Security/IT policies, Acceptable Use Agreements, Mobile Phone/Device procedures, Remote Education arrangements and relevant curriculum policies.

Appendix

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will use school technology safely, responsibly and for learning. I understand that the school may use filtering and monitoring to help keep everyone safe.

I will keep passwords private and use only my own account.

I will protect personal information such as my full address, phone number, passwords and location.

I will be kind and respectful when communicating online.

I will tell a trusted adult if something online worries, upsets, pressures or confuses me.

I will not deliberately search for harmful or inappropriate material or try to bypass school safety controls.

I will not take, share or alter images, video or audio of another person without permission.

I will not pretend to be another person or use technology or AI to bully, embarrass, threaten or deceive someone.

I will only use AI tools when a teacher has said I may do so and will follow the rules for that activity.

I will not put personal, private or safeguarding information into an AI tool.

I understand that AI can make mistakes or create things that look real but are not real, so I will check information and ask an adult when unsure.

I will be honest about my own work and will not use AI or other technology to make work appear to be mine when it is not permitted.

Parent/carer agreement: I support the school's expectations for safe and responsible use of technology. I understand that filtering and monitoring are used as safeguarding measures and will support my child to report concerns and use online services safely.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date: