



Online Safety Policy

Ratified by Governing Body

Review: September 2027

PURPOSE AND SCOPE

Herrick Primary School recognises that safeguarding children includes keeping them safe online. Online safety is an integral part of safeguarding and child protection and applies to all pupils, staff, governors, volunteers, visitors and where relevant, parents and carers.

This policy applies to school-owned and school-managed devices, networks, cloud services, educational applications, communication tools, generative artificial intelligence (AI) and online activity connected with school business, whether undertaken on or off site.

This policy should be read alongside the school's Child Protection and Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct, Data Protection Policy, Social Media Policy, acceptable use agreements and relevant local authority procedures.

LEGAL AND STATUTORY FRAMEWORK

The school will have regard to current legislation and statutory guidance applicable in England, including:

- Children Act 1989 and Children Act 2004.
- Education Act 2002, including the duty to safeguard and promote the welfare of children.
- Education and Inspections Act 2006.
- Equality Act 2010.
- Counter-Terrorism and Security Act 2015 and the Prevent duty.
- Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025.
- Voyeurism (Offences) Act 2019.
- Online Safety Act 2023, where relevant to the wider online-safety environment.
- Keeping Children Safe in Education (KCSIE) 2026, in force from 1 September 2026.
- Working Together to Safeguard Children and current DfE safeguarding guidance.
- DfE filtering and monitoring standards, cyber security standards, data-protection guidance and guidance on generative AI in education.

Where legislation or statutory guidance changes, the school will apply the current requirements even if this policy has not yet reached its scheduled review date.

PRINCIPLES

- Children should be able to benefit from technology while being protected from illegal, inappropriate and harmful content, contact, conduct and commercial risks.
- Online safeguarding concerns will be treated as safeguarding concerns, not solely as behaviour or IT issues.
- Online abuse can occur inside or outside school and can involve pupils, adults or unknown individuals.
- Filtering and monitoring are safeguards, but do not replace effective supervision, education, professional curiosity or reporting.
- Provision will take account of age, SEND, EAL, vulnerability, curriculum need and the school's local risk profile.

ROLES AND RESPONSIBILITIES

GOVERNING BODY

- Has strategic responsibility for ensuring appropriate filtering and monitoring arrangements are in place.
- Receives assurance that online-safety arrangements, staff training and filtering/monitoring reviews are effective.
- Ensures this policy is reviewed at least annually and following significant changes or incidents.

HEADTEACHER AND SENIOR LEADERS

- Ensure this policy is implemented and resourced.
- Ensure staff understand their responsibilities and receive appropriate training.
- Ensure new technology and services are appropriately risk assessed before use.

DESIGNATED SAFEGUARDING LEAD (DSL)

- Takes lead responsibility for safeguarding and child-protection concerns arising online.
- Works with IT support and senior leaders on filtering and monitoring.
- Ensures alerts and concerns are assessed, recorded and acted upon in line with safeguarding procedures.
- Ensures staff know how and when to report online-safety concerns.

ONLINE SAFETY / COMPUTING LEAD

- Supports curriculum provision, staff awareness and policy implementation.
- Works with the DSL and IT support to identify emerging risks and appropriate educational responses.

IT SUPPORT

- Maintains technical safeguards, filtering, monitoring, account security and cyber-security controls.

- Reports safeguarding concerns arising through technical systems promptly to the DSL.
- Does not make safeguarding decisions independently of the DSL.

ALL STAFF

- Maintain appropriate supervision of pupils using technology.
- Follow the Staff Acceptable Use Agreement and Staff Code of Conduct.
- Report safeguarding concerns immediately through the school's agreed safeguarding route.
- Do not conduct their own investigation into a safeguarding concern unless directed by the DSL.

THE FOUR AREAS OF ONLINE RISK

The school's approach will address the four broad areas identified in KCSIE:

Area	Examples
Content	Illegal, inappropriate or harmful material, including sexual content, pornography, violence, misogyny, self-harm content, extremist material, misinformation and harmful AI-generated content.
Contact	Harmful interaction with other users, including adults posing as children, grooming, exploitation and inappropriate communication.
Conduct	Personal online behaviour that increases risk or causes harm, including cyberbullying, sharing nudes or semi-nudes, sexual harassment, abuse, impersonation and misuse of technology.
Commerce	Online gambling, inappropriate advertising, scams, phishing and financial exploitation.

FILTERING AND MONITORING

The school will maintain filtering and monitoring arrangements appropriate to its pupils, staff, curriculum and safeguarding risk profile.

- Filtering and monitoring provision will be formally reviewed at least once every academic year by senior leadership, the DSL, IT support and the responsible governor.
- Checks will be recorded and will include school-managed devices and services, relevant locations, user profiles and new devices/services before deployment.

- Filtering will seek to block illegal, inappropriate and harmful content without unreasonably restricting teaching and learning.
- Monitoring will enable concerns to be identified and escalated promptly. High-risk safeguarding alerts will be handled urgently.
- All staff will understand that filtering does not replace supervision and will report unsuitable material, filtering failures or unreasonable restrictions.
- Users will be informed that school systems and devices may be filtered and monitored.
- Monitoring data will only be accessible to authorised personnel and handled in accordance with data-protection requirements.
- A Data Protection Impact Assessment (DPIA) will be completed where required before introducing or significantly changing monitoring technology.
- The school will consider whether filtering and monitoring can address dynamic, personalised and AI-generated content.

GENERATIVE ARTIFICIAL INTELLIGENCE (AI)

The school recognises the educational opportunities and safeguarding, accuracy, copyright, bias and data-protection risks associated with generative AI.

- Only school-approved AI tools may be used for school business (Gemini and Canva).
- Age restrictions and terms of service must be followed.
- Pupil use of generative AI in school will only take place where authorised, age appropriate and appropriately supervised.
- Personal, special-category, confidential or safeguarding information must not be entered into an AI system unless the school has explicitly approved that processing and the relevant data-protection requirements have been met.
- Staff remain professionally responsible for checking the accuracy, suitability, bias and safety of AI-generated material.
- AI must not replace professional safeguarding judgement or decision-making.
- AI-generated images, audio, video or text used to bully, impersonate, sexualise, deceive or harm others will be treated as an online-safety and/or safeguarding concern.
- Staff and pupils must follow school expectations regarding acknowledgement of AI-assisted work where applicable.

DATA PROTECTION, PRIVACY AND IMAGES

- Personal data will be processed lawfully, fairly, transparently and securely in accordance with UK data-protection law and school policies.
- School data must only be stored or shared using authorised systems.
- Images and videos of pupils will be captured, stored and published only in accordance with the school's safeguarding, privacy and consent arrangements.

- Personal devices must not be used to photograph or record pupils unless an exceptional arrangement has been explicitly authorised by the Headteacher and complies with school policy.
- Filtering and monitoring privacy information will explain what is monitored, why, who can access alerts/reports and relevant retention arrangements.

CYBER SECURITY

- Users must protect passwords and accounts and use multi-factor authentication where provided.
- Users must not deliberately bypass filtering, monitoring or security controls, including through VPNs, proxies or unauthorised software.
- Suspicious emails, phishing attempts, malware, compromised accounts, lost devices and suspected data breaches must be reported promptly.
- Software, browser extensions and applications may only be installed where authorised.
- School information must not be stored on unauthorised personal devices, personal cloud storage or unencrypted removable media.

CHILD-ON-CHILD ONLINE ABUSE

Online child-on-child abuse may include cyberbullying, sexual harassment, coercion, threats, non-consensual sharing of images, sharing nudes or semi-nudes, abuse based on protected characteristics, misogynistic or discriminatory abuse, impersonation and harmful online challenges.

Incidents will be considered through a safeguarding lens. The school will not dismiss abusive online behaviour as banter or an inevitable part of growing up.

SHARING NUDES AND SEMI-NUDES AND SEXUAL IMAGERY

Any concern involving the creation, request, possession or sharing of nude or semi-nude images by children will be reported to the DSL immediately and managed in accordance with KCSIE, the school's safeguarding procedures and current national guidance. Staff must not forward, copy, print or unnecessarily view such imagery. The DSL will determine appropriate safeguarding action and whether external agencies should be involved.

ONLINE RADICALISATION AND EXTREMISM

The school recognises that children and adults may be exposed to extremist or terrorist material and radicalising influences online. Concerns will be reported to the DSL and considered under the school's safeguarding and Prevent procedures. Filtering and monitoring arrangements will support, but not replace, professional vigilance.

ONLINE SAFETY EDUCATION

Online safety will be taught in an age-appropriate and progressive way through Computing, PSHE, assemblies and other curriculum opportunities. Pupils will learn how to recognise risk, protect personal information, communicate respectfully, identify unreliable information and scams, use AI safely, seek help and report concerns.

EMERGING AND SPECIFIC ONLINE RISKS

The school recognises that online risks change rapidly. The following risks will be addressed through safeguarding procedures, curriculum teaching, filtering and monitoring, staff training and proportionate responses.

ONLINE BULLYING AND HARASSMENT: Includes repeated or one-off harmful messages, exclusion, humiliation, threats, discriminatory abuse, pile-ons, impersonation and the use of images, video, audio or AI-generated material to harm another person.

GROOMING AND EXPLOITATION: Includes attempts to build trust with a child for sexual, criminal, financial or other exploitation; requests for secrecy; moving conversations to private platforms; requests for images; gifts or incentives; threats; coercion and blackmail.

SEXTORTION AND SEXUAL COERCION: Any threat to share intimate or fabricated sexual imagery, or demand for money, further images or other actions, will be treated as an urgent safeguarding concern. Pupils will be reassured that they should report rather than comply with demands.

DEEPFAKES AND AI-GENERATED IMAGERY: Creating, altering or sharing realistic fake images, video, audio or text to sexualise, bully, impersonate, deceive or humiliate a pupil or member of staff may constitute a serious safeguarding, behaviour and/or criminal concern.

CYBERFLASHING AND UNWANTED SEXUAL CONTENT: Unsolicited sexual images, sexualised messages or exposure to sexual content will be reported and managed through safeguarding procedures.

IMPERSONATION, CATFISHING AND FAKE ACCOUNTS: Pretending to be another person, creating fake profiles or using another person's identity to deceive, contact or harm others will be addressed as an online-safety concern.

DOXXING AND MALICIOUS DISCLOSURE: Publishing or threatening to publish another person's private or identifying information, location or contact details without permission will be treated seriously.

HATE AND DISCRIMINATORY ABUSE: Online abuse connected to disability, race, religion or belief, sex, sexual orientation, gender reassignment or other protected characteristics will be addressed under safeguarding, behaviour and equality duties.

DANGEROUS CHALLENGES, HOAXES AND VIRAL TRENDS: Pupils will be taught to recognise and report challenges or trends that encourage unsafe, harmful, illegal or humiliating behaviour.

MISINFORMATION, DISINFORMATION AND MANIPULATED MEDIA: Pupils will be taught that online information, images, videos, search results and AI-generated summaries may be inaccurate, misleading, manipulated or fabricated and should be checked against reliable sources.

GAMING AND IN-GAME COMMUNICATION: Risks may include contact with unknown users, bullying, inappropriate language/content, grooming, scams, loot-box or purchase pressure and attempts to move communication to private platforms.

LIVESTREAMING, GEOTAGGING AND LOCATION SHARING: Pupils will be taught that livestreams, photographs, metadata, backgrounds, uniforms and location services can reveal personal information or a person's location.

SUPPORTING PUPILS WITH SEND, EAL AND ADDITIONAL VULNERABILITIES

The school will adapt online-safety education, supervision and safeguards to meet individual needs. Risk assessment will consider age, SEND, communication needs, EAL, prior safeguarding concerns and other vulnerabilities.

PARENTS AND CARERS

The school will work in partnership with parents and carers by sharing relevant guidance, communicating emerging concerns where appropriate, and encouraging consistent messages about safe and responsible technology use.

1. Parents/carers will be informed where appropriate, unless doing so would increase risk or prejudice an investigation.

STAFF PROFESSIONAL BOUNDARIES ONLINE

- Staff must use approved school communication channels for school business.
- Staff must not communicate privately with current pupils through personal social-media or messaging accounts.
- Staff must not share pupil information through unauthorised personal messaging, email, cloud or AI services.
- Staff must maintain professional standards online and must not post content that breaches confidentiality, safeguarding duties or professional conduct expectations.

INCIDENTS, SANCTIONS AND SUPPORT

Breaches by pupils will be addressed proportionately in accordance with the Behaviour Policy while safeguarding needs are considered. Staff breaches may be addressed under the Staff Code of Conduct and disciplinary procedures. Suspected criminal activity will be referred to the appropriate authority where required.

REVIEW

This policy will be reviewed at least annually and sooner following significant safeguarding incidents, material changes to legislation or statutory guidance, significant cyber incidents, or substantial changes to the school's technology, AI, filtering or monitoring provision.

KEY SAFEGUARDING AND ONLINE SAFETY CONTACTS

Role / responsibility	Name	Contact numbers	
Headteacher	Sima Odedra	0116 2665656	Office@herrick.leicester.sch.uk
Designated Safeguarding Lead (DSL)	Arzu Aydin	0116 2665656	Office@herrick.leicester.sch.uk
Deputy DSL(s)	Sima Odedra, Shani Kaur, Firza Suleman.	0116 2665656	Office@herrick.leicester.sch.uk
Designated Safeguarding Governor	Steve Martin	0116 2665656	Office@herrick.leicester.sch.uk
Data Protection Lead / DPO	Firza Suleman	0116 2665656	Office@herrick.leicester.sch.uk
Filtering, Monitoring & Online Safety Lead	Arzu Aydin	0116 2665656	Aaydin@herrick.leicester.sch.uk
IT / Technical Support Provider	MTS Provider	0116 2665656	Office@herrick.leicester.sch.uk
Computing Lead	Monica Nai	0116 2665656	Office@herrick.leicester.sch.uk

EXTERNAL AGENCY CONTACT DETAILS

LADO (Local Authority Designated Officer)	0116 454 2440 - Lado-allegations-referrals@leicester.gov.uk
NSPCC	https://learning.nspcc.org.uk/
Operation Encompass	0204 513 9990 Available Monday to Friday 8am-1pm

LCC Early Help	0116 454 1004

REPORTING AND RESPONDING TO CONCERNS

2. Any member of staff who identifies an online safeguarding concern must report it promptly using the school's safeguarding procedure.
3. Staff should preserve relevant information but must not undertake their own investigation, search a pupil's private online accounts or seek technical evidence unless directed through an authorised process.
4. The DSL or deputy will assess risk and decide the safeguarding response.
5. Referrals to Children's Social Care, police, Prevent/Channel, LADO or other agencies will be made where appropriate.
6. Actions, decisions and outcomes will be recorded in accordance with safeguarding and data-protection procedures.

APPENDIX A - ONLINE SAFETY INCIDENT PATHWAY



CONCERN IDENTIFIED

A potential safeguarding or safety concern is noticed or disclosed



MAKE SITUATION SAFE

Ensure immediate safety for everyone; do not investigate yet



REPORT TO DSL

Immediately notify the Designated Safeguarding Lead or Deputy



DSL ASSESSES RISK

The DSL evaluates the information to determine the level of risk



RECORD CONCERN

Accurately document the concern, facts, and initial actions taken



EXTERNAL REFERRAL

If appropriate, contact external authorities like social care or emergency services



SUPPORT AFFECTED INDIVIDUALS

Provide ongoing care, reassurance, and support to children and staff



REVIEW CONTROLS & POLICY

Evaluate policies, training, and systems to prevent future issues

