# Heritage Park Primary School

# Online Safety Policy

| | |
|---|---|
| **Approved by:** | Senior Leadership Team |
| **Last reviewed on:** | March 2026 |
| **Next review due by:** | October 2027 |

# Heritage Park Primary School
# Online Safety Policy

## Aims

Heritage Park Primary School aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors, including more vulnerable pupils who may be at greater risk of harm online than others.
- Deliver an effective approach to online safety that empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene, and escalate incidents where appropriate.
- Ensure alignment with the expectations introduced through Keeping Children Safe in Education (KCSIE) 2025–2026, which expands online content risk categories to include *misinformation, disinformation, and conspiracy theories*.
- Meet new duties introduced by the Online Safety Act, including expectations for schools to assess risks relating to harmful online content, maintain transparent content management practices, and uphold strengthened safeguarding duties relating to harmful or age-inappropriate content online.

## Legislation and Guidance

This policy is based on up-to-date statutory legislation and guidance, including:
Department for Education (DfE) statutory guidance

- Keeping Children Safe in Education (KCSIE) 2025
- Teaching Online Safety in Schools (DfE)
- Preventing and Tackling Bullying (including cyberbullying)
- Searching, Screening and Confiscation guidance

Other statutory and regulatory frameworks

- Online Safety Act 2023, fully in force from August 2025, which places legal duties on platforms to protect children from illegal and harmful content, and requires effective age assurance systems designed to prevent access to pornography, self-harm content, and other harmful materials. The Act also requires schools to maintain robust safeguarding processes and ensure transparency when responding to harmful content incidents.
- Education Act 1996 (as amended)
- Education and Inspections Act 2006
- Equality Act 2010
- Education Act 2011, giving teachers powers to search for and delete inappropriate material on electronic devices where a good reason exists.

Additional Relevant Guidance

- Working Together to Safeguard Children (2026 Update): strengthened expectations for multi-agency working, inclusive practice, and recognition of coercive or less visible harms.
- Prevent Duty Guidance and the Counter-Terrorism and Security Act 2015, updated with new government guidance and risk indicators for radicalisation relevant to online spaces.

## The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk, updated to reflect the current statutory definitions under KCSIE 2025:

**Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news (*misinformation, disinformation and conspiracy theories)*, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

**Contact** – being subjected to harmful online interaction with other users, such as peer pressure, adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

**Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as creating, sending or receiving explicit images (including consensual or non-consensual sharing of nudes and semi-nudes), online bullying, sharing explicit images of others, *AI-generated abuse (e.g., deepfakes)*

**Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

## Roles and responsibilities

### Governing Body

The governing body has strategic oversight of this policy and ensures effective implementation. It must:

- Ensure online safety is embedded throughout the school's safeguarding approach and all staff receive online safety training as part of safeguarding, with updates at least annually, in line with expectations for regularly refreshed knowledge.
- Ensure roles and responsibilities for managing filtering and monitoring are clearly assigned and the school's systems meet the DfE Filtering and Monitoring Standards.
- Ensure harmful or inappropriate content is effectively blocked without disrupting learning and hold regular meetings (via the safeguarding governor) to review online safety issues, training needs and incident patterns.
- Ensure teaching about online safety is adapted for vulnerable pupils and those with SEND, recognising that a "one size fits all" approach may not be appropriate.
- Maintain awareness of duties under the Online Safety Act, including risks from harmful content, reporting expectations, and the strengthened duty on schools to monitor exposure to unsafe material.

The safeguarding governor also acts as the online safety governor.

### Headteacher

The headteacher ensures that:

- Staff understand this policy and implement it consistently.
- Online safety is embedded across the school's safeguarding culture.
- The governing body receives required information about online safety, filtering/monitoring, and emerging risks.

### Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for online safety, in line with KCSIE. Responsibilities include:

- Ensuring all staff understand and apply this policy.
- Working with the safeguarding governor to regularly review policy and procedures, reflecting updates in statutory guidance (e.g., AI risk, misinformation, cyber security).

- Leading on understanding and overseeing filtering and monitoring systems.
- Working with the ICT technician and computing lead to ensure technical systems are secure and effective.
- Ensuring all online safety incidents (including cyber-bullying) are logged and managed appropriately.
- Recognising AI-generated abuse (e.g., deepfake imagery) as a safeguarding concern and ensuring staff understand how to identify and report this.
- Liaising with external agencies when needed.
- Delivering staff training on online safety/safeguarding and providing updates at least annually, including new risks identified in statutory guidance.

**ICT Technician**
The ICT technician is responsible for:
- Implementing secure filtering and monitoring systems in accordance with DfE standards and reviewing them at least annually.
- Ensuring all ICT systems are secure, updated, protected from malware, and compliant with strengthened cyber-security expectations
- Conducting monthly security checks.
- Blocking access to dangerous sites and preventing unsafe downloads where possible.
- Logging online safety incidents and supporting appropriate resolution.
- Supporting staff when technical issues affect filtering and monitoring.

**All Staff and Volunteers**
All staff, contractors, and volunteers must:
- Understand and follow this policy and the acceptable use rules.
- Ensure pupils follow their acceptable use agreements.
- Report any filtering or monitoring failures immediately to the headteacher, who will inform the ICT technician.
- Seek ICT advice and headteacher approval before bypassing filters for approved educational purposes.
- Log and help manage online safety incidents and cyber-bullying with the DSL.
- Respond to concerns about sexual violence/harassment (online or offline) with an “it could happen here” approach, as required by KCSIE.
- Understand new and emerging online harms, including misinformation, disinformation, and AI-generated risks

**Parents/Carers**
Parents/carers are expected to:
- Raise any questions or concerns about this policy with school staff.
- Ensure their child has read and agreed to the pupil acceptable use terms.
- Use recommended organisations (e.g., UK Safer Internet Centre, Childnet) for guidance on online safety.

**Visitors and Community Users**
Visitors and community users accessing school ICT systems or the internet will be made aware of this policy and, where appropriate, required to read and follow the acceptable use expectations.

## Educating Pupils About Online Safety

Online safety is taught throughout the curriculum.

**Key Stage 1**

Pupils learn to:

- Use technology safely and respectfully.
- Keep personal information private.
- Know where to go for help if they feel worried about online content or contact.

**Key Stage 2**

Pupils learn to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable online behaviour.
- Identify different ways to report concerns.

**By the End of Primary School, Pupils Will Know:**

- People may behave differently online, including pretending to be someone else.
- Respectful behaviour applies online as well as offline, even when anonymous.
- Rules for staying safe, recognising risks and harmful content, and reporting concerns.
- How to critically question online friendships and information, including risks from people they have never met.
- How information/data is shared and used online.
- What appropriate boundaries look like in online relationships.
- How to respond safely to unfamiliar adults online.

Online safety is also reinforced through PSHCE and other subjects. Teaching may be adapted for vulnerable pupils, pupils with SEND, and those who have experienced abuse.

## Educating Parents/Carers

- The school promotes online safety to parents/carers through letters, our website, and other communications.
- Parents/carers should raise any queries with staff or the headteacher.
- Support is signposted to trusted organisations (e.g. UK Safer Internet Centre, Childnet).

## Cyber-Bullying

**Definition**

Cyber-bullying occurs online (e.g., messaging apps, gaming sites) and involves intentional, repeated harm where there is an imbalance of power.
(See behaviour and anti-bullying policies.)

**Prevention and Response**

The school will:

- Ensure pupils understand what cyber-bullying is and how to report concerns.
- Discuss cyber-bullying openly, including causes, forms and consequences.
- Use PSHCE and other curriculum opportunities to reinforce learning.
- Provide staff training on cyber-bullying as part of safeguarding.
- Share information with parents/carers on signs, reporting, and support.

For specific incidents:

- Behaviour policy procedures will be followed.
- The school will act to contain and address harmful or illegal material.
- The DSL will involve the police where material is suspected to be illegal and liaise with external agencies when needed.

**Examining Electronic Devices**

Authorised staff may search and confiscate a device if they reasonably suspect it:

- Poses a risk,
- Is banned under school rules, or
- May contain evidence of an offence.

Before searching, staff will assess urgency, consider risk, explain the process to the pupil, and seek cooperation. Authorised staff may examine or erase data where they have a *good reason* to do so. A "good reason" includes reasonable suspicion that the device has been or could be used to:

- Cause harm,
- Disrupt the safe environment, or
- Commit an offence.

If inappropriate material is found:

- Staff will liaise with the DSL to determine the response.
- If material may be evidence of a criminal offence, it will not be deleted and will be passed to the police.

Where staff suspect a device contains an indecent image of a child:

- They **must not** view the image.
- The device will be confiscated and immediately passed to the DSL.
- The DSL will act in line with DfE searching guidance and UKCIS *Sharing Nudes and Semi-Nudes* guidance.

Searching will be carried out in line with:

- The latest DfE guidance on searching, screening and confiscation,
- UKCIS guidance on nudes/semi-nudes,
- The school behaviour policy.

Complaints will follow the school's complaints procedure.

**Artificial Intelligence (AI)**

The school recognises both the educational value and risks of AI tools.
AI can be misused to harm others, including creating deepfakes or hoax content.

- Any AI-related bullying will be dealt with under the Anti-Bullying and Behaviour Policies.
- Staff must be aware of risks associated with emerging AI tools.

**Acceptable Use of the Internet**

- All pupils, staff, volunteers, governors, parents/carers and relevant visitors must sign an Acceptable Use Agreement.

- School internet must be used only for educational purposes or role-related duties.
- Use is monitored and access restricted using the school's filtering systems.
- Further details are in Appendices 1–3.

**Pupils Using Mobile Devices**

- Pupils are not permitted to bring mobile devices to school.
- In exceptional circumstances, with prior agreement from the Senior Leadership Team, a pupil may bring a phone but must hand it in to the school office for the day.

**Staff Using Work Devices Outside School**

Staff must keep work devices secure by:

- Using strong passwords,
- Ensuring drives are encrypted,
- Enabling automatic screen-locking,
- Updating software regularly,
- Using anti-virus/anti-spyware,

Work devices must only be used for work activities and in line with the Acceptable Use Agreement. Staff must report any security concerns to the headteacher and ICT technician.

**Responding to Misuse**

- Where a pupil misuses the school's ICT systems or internet, the school will follow the behaviour and acceptable use policies. Responses will be proportionate to the circumstances, nature and seriousness of the incident.
- Where a staff member misuses ICT systems or the internet — including misuse of a personal device amounting to misconduct — the matter will be addressed under the staff disciplinary procedures. Again, actions will be proportionate to the case.
- The school will consider referring serious or potentially illegal incidents to the Local Authority Designated Officer (LADO) or the police.

**Training**

- All new staff receive training on online safeguarding as part of induction.
- All staff receive safeguarding refresher training, including online safety, at least annually, with additional updates provided when necessary (e.g., by email or staff meetings).

Through this training, staff will understand that:

- Technology is a major factor in many safeguarding issues, and children may be at risk of online abuse.
- Children can abuse peers online through:
    - Abusive, harassing or misogynistic messages
    - Non-consensual sharing of nude or semi-nude images/videos
    - Sharing abusive images or pornography

Training will help staff to:

- Recognise signs of online abuse
- Support pupils in recognising risks and making safe choices
- Help pupils build healthy, long-term digital behaviours

The DSL and deputies complete child protection training (including online safety) at least every 2 years and refresh their knowledge at least annually.

Staff training needs will be assessed through the use of an audit tool (Appendix 4).

Governors receive training on online safety as part of their safeguarding responsibilities.

**Monitoring Arrangements**

- The DSL records online safety-related behaviour and safeguarding concerns using the school's incident log (Appendix 5).
- This policy is reviewed annually by the Senior Leadership Team and shared with all staff and the governing body after each review.

**Appendix 1: EYFS and KS1 Acceptable Use Agreement (Pupils and Parents/Carers)**

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS | |
|---|---|
| **Name of pupil:** | |
| **When I use school computers, tablets or the internet, I will:**<br><br>• **Ask an adult before using any device or going online.**<br>• **Only use websites/apps that an adult has checked or approved.**<br>• **Tell an adult straight away if:**<br>  ○ **I see something upsetting or unsafe,**<br>  ○ **Someone I don't know contacts me,**<br>  ○ **I click on something by mistake.**<br>• **Be kind online and use polite words.**<br>• **Look after school equipment and report anything broken.**<br>• **Use only my own username and password and keep them private.**<br>• **Never share my personal information (my name, address, school, phone number) unless a teacher says it is safe.**<br>• **Save my work in the right place and ask before printing.**<br>• **Log out when I've finished.**<br>**I know the school checks what I do online to help keep me safe.** | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer agreement**:<br>**I agree my child may use the school's ICT and internet under supervision and I will help them follow these rules.** | |
| **Signed (parent/carer):** | **Date:** |

**Appendix 2: KS2 Acceptable Use Agreement (Pupils and Parents/Carers)**

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS | |
|---|---|
| **Name of pupil:** | |
| When using school ICT or the internet, I will:<br>• Use technology safely, respectfully and *only for learning*.<br>• Use it only with permission or when supervised by an adult.<br>• Keep my usernames and passwords safe and private.<br>• Protect my personal information.<br>• Tell an adult immediately if I see anything worrying, harmful or inappropriate<br>• Log off when finished.<br>I will **not**:<br>• Access inappropriate sites (including social media, chat rooms or gaming sites) unless part of a teacher-approved lesson.<br>• Open email attachments or click links without checking with a teacher.<br>• Use rude, bullying, hateful or discriminatory language online (reflecting KCSIE's inclusion of misogyny/hate as online harms).<br>• Create or share inappropriate, offensive, obscene or harmful content.<br>• Use someone else's login details.<br>• Arrange to meet anyone from online without permission and supervision.<br>• Create or share AI-generated, edited or "deepfake" images of others.<br>**If I bring a mobile device to school (rare exceptions only):**<br>• I will hand it to the office as required.<br>• I will not use it during the school day without permission.<br>• I will not access inappropriate sites or apps.<br>I understand the school monitors online activity. | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer's agreement:** 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:** |

**Appendix 3: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)**

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS | |
|---|---|
| When using school ICT systems or work devices (in or out of school), I will:<br>• Use them only for professional and educational purposes.<br>• Follow safeguarding expectations relating to online risks, including misinformation/disinformation and harmful content categories added in KCSIE 2025.<br>• Be aware that cyber security standards are part of statutory compliance<br>I will not:<br>• Access, create, share or link to inappropriate, violent, illegal or pornographic material.<br>• Use ICT in any way that harms the school's reputation.<br>• Access social networking or chat services on school systems unless required for teaching and approved.<br>• Use abusive, discriminatory or inappropriate language online.<br>• Install unauthorised software or connect unapproved devices.<br>• Share passwords or use others' login credentials.<br>• Take photographs of pupils without permission (for non-staff).<br>• Share confidential or sensitive information improperly.<br>• Access or share data I am not authorised to access.<br>I understand:<br>• The school monitors ICT use in line with safeguarding and the Online Safety Act, which requires risk assessment and monitoring of harmful content exposure.<br>• I must report any harmful or upsetting content disclosed by a pupil immediately to the DSL.<br>• AI-generated misuse (including deepfakes) is treated as a safeguarding matter<br>I will keep devices secure and follow the data protection policy. | |
| **Please sign and print name:** | **Date:** |

**Appendix 4: Online Safety Training Needs – Self-Audit Tool**

| ONLINE SAFETY TRAINING NEEDS AUDIT | |
|---|---|
| **Name of staff member/volunteer:** | **Date**: |
| **Question** | **Yes/No (add comments if necessary)** |
| Do you know who has lead responsibility for online safety in school? | |
| Are you aware of key online harms including those added in KCSIE 2025 (misinformation, disinformation, conspiracy theories)? | |
| Do you understand how pupils may abuse peers online (including AI-generated deepfakes as recognised in KCSIE 2026 draft)? | |
| Do you know what to do if a pupil reports online harm? | |
| Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? | |
| Do you understand the school's filtering & monitoring systems and the DfE standards? | |
| Do you know your role in reporting failures in filtering/monitoring? | |
| Do you change your ICT passwords regularly? | |
| Do you understand the school's approach to cyber-bullying and online behaviour? | |
| Do you require further training in any aspect of online safety? | |

**Appendix 5: Online Safety Incident Report Log**

| ONLINE SAFETY INCIDENT LOG | | | | |
|---|---|---|---|---|
| **Date** | **Where the incident took place/Platform** | **Description of incident (include whether misinformation, harmful content, cyber-bullying, AI-generated content, etc.)** | **Action taken** | **Name of staff member recording the incident** |
| | | | | |