



HIPPINGS METHODIST PRIMARY SCHOOL



ONLINE SAFETY POLICY

“As a family we do our best with God in our hearts.”

“I can do all things through Christ who strengthens me.”

Date approved / reviewed	September 2026
Checked by	Mrs T Westwell, Headteacher and DSL; Mrs M Hunter, Deputy Headteacher and DSL
Chair of Governors	Mrs M Gardner
Next review	September 2027, or sooner where guidance, technology, safeguarding risks or school arrangements change

1. Purpose

The purpose of this policy is to safeguard and protect all members of the Hippings Methodist Primary School online community by providing a clear framework for a safe, effective and responsive online-safety culture.

The policy applies to all staff, pupils, volunteers, governors, parents/carers, visitors and other users who access school digital technology, systems, networks or online services, whether on or away from the school site.

Online safety is part of the school's wider safeguarding arrangements and must be read alongside the school's Safeguarding and Child Protection Policy, Behaviour Policy, Acceptable Use Policy, Data Protection/Privacy Policy, Mobile Phone/Smart Technology arrangements and other relevant school procedures.

2. Aims

At Hippings Methodist Primary School, we aim to help every pupil and adult to:

- feel safe and confident when using digital technology;
- know who to speak to when they feel unsafe or worried online;
- know how to report online abuse, bullying or other concerns;
- understand how to use the internet, devices and online services responsibly and safely;
- recognise online risks at an early stage and know how to respond;
- protect personal information, accounts, passwords and digital identity;
- understand how to block, mute, report and remove unwanted contacts, accounts or messages where appropriate;
- understand that online behaviour can have real-world safeguarding, emotional, legal and disciplinary consequences;
- develop critical thinking skills so that they can question the reliability, accuracy and purpose of online information;

- understand emerging risks, including generative artificial intelligence (AI), deepfakes, scams and misleading or manipulated content.

3. Legislation and statutory guidance

This policy is informed by and should be read alongside current statutory and non-statutory guidance applicable to schools in England, including:

- Keeping Children Safe in Education (KCSIE) 2026;
- Working Together to Safeguard Children 2026;
- Department for Education (DfE) Meeting Digital and Technology Standards in Schools and Colleges – Filtering and Monitoring: Core Standard;
- DfE Generative Artificial Intelligence (AI) in Education guidance;
- DfE Generative AI: Product Safety Standards;
- DfE Cyber Security Standards for Schools and Colleges;
- Prevent Duty guidance;
- UK GDPR and the Data Protection Act 2018;
- relevant UK Council for Internet Safety (UKCIS), Safer Internet Centre and National Cyber Security Centre guidance.

The policy will be reviewed when statutory guidance, DfE standards, technology, school systems or safeguarding risks change.

4. Roles and responsibilities

4.1 Headteacher, Senior Leadership Team and Governing Body

- Ensure online safety is embedded within the school's whole-school safeguarding culture.
- Ensure pupils are provided with a safe environment in which to learn and develop, including protection from online harm.
- Ensure appropriate filtering and monitoring systems are in place, understood and regularly reviewed.
- Ensure staff receive appropriate safeguarding and online-safety information and training.
- Ensure robust reporting, recording, escalation and referral arrangements are in place.
- Ensure online-safety policies, systems and processes are kept under continual review and have a positive impact on pupils.
- Ensure appropriate risk assessments are completed when new technology, online services or significant changes are introduced.
- Provide governors with appropriate assurance about filtering, monitoring, cyber security, online-safety education and significant safeguarding incidents.

4.2 DSL and Deputy DSLs

- Take responsibility for online safeguarding as part of the school's wider safeguarding arrangements.
- Ensure online-safety concerns are recorded, assessed, referred and followed up through the school's safeguarding procedures.
- Work with SLT, the computing lead, IT support and relevant external providers to review online risks and technical safeguards.

- Ensure staff and pupils know how and where to report concerns.
- Ensure online-safety education is age appropriate and responsive to emerging risks.
- Review relevant monitoring alerts and ensure high-risk safeguarding concerns are escalated immediately.
- Maintain appropriate training and professional knowledge.

4.3 Teachers and support staff

- Model safe, respectful and professional use of technology.
- Follow all school safeguarding, online-safety, acceptable-use, data-protection and device policies.
- Use school-approved systems for professional communication with pupils.
- Report safeguarding concerns promptly through CPOMS and notify a DSL as soon as possible.
- Know how to recognise signs of online abuse, bullying, exploitation, harmful content and other online harm.
- Supervise pupils appropriately when they use online services and intervene where necessary.
- Teach and reinforce online-safety messages across the curriculum.
- Keep up to date with relevant online-safety developments, including AI.

4.4 Technical support

- Maintain secure school ICT infrastructure and support the school in meeting relevant DfE digital and cyber-security standards.
- Maintain and update filtering and monitoring systems in partnership with the school and service provider.
- Support secure account management, authentication, software updates and appropriate access controls.
- Escalate technical failures, vulnerabilities and safeguarding-related technical concerns promptly.
- Maintain appropriate technical knowledge and liaise with Lancashire Education Digital Services/approved IT support.

4.5 Pupils

- Use technology safely, respectfully and responsibly.
- Follow the school's Acceptable Use Policy and instructions from staff.
- Protect passwords and personal information and never share another person's personal information without permission.
- Report anything online that makes them feel unsafe, worried or uncomfortable to a trusted adult.
- Treat others respectfully online and offline.
- Understand that online activity can be permanent or difficult to remove and may have consequences.

4.6 Parents and carers

- Support children to use internet-enabled devices and online services safely and appropriately.
- Be familiar with the school's online-safety and Acceptable Use arrangements.
- Raise online-safety concerns with the school where appropriate.
- Support the school's expectations around age restrictions, privacy, online communication and respectful behaviour.
- Access information and guidance shared by the school and trusted national online-safety organisations.

5. Filtering and monitoring

5.1 School provision

Hippings Methodist Primary School receives its broadband and online services through Lancashire County Council Education Digital Services. The school's broadband service includes web filtering based on Netsweeper.

- Education-focused web filtering is provided to support safe, filtered and logged web access for staff and pupils.
- Filtering policies can be differentiated according to username, group membership or IP range.
- The school can manage which websites and categories of websites it allows or blocks, subject to the provider's controls and safeguarding requirements.
- Monitoring and reporting on web access are available, including configurable reports.
- Illegal content identified through the provider's arrangements remains blocked and cannot be overridden by school staff.
- Filtered web access is provided to devices connected through the school service.
- Filtering and monitoring arrangements will be reviewed when new technologies, services, devices or safeguarding risks are introduced.

The school's provider is Lancashire Education Digital Services. The school should retain current provider information and service documentation separately where links or technical specifications change.

5.2 OnGuard monitoring and alerting

The school's Broadband and Online Services bundle includes OnGuard, a monitoring and alerting service. The school understands the service to provide AI-detected and human-verified digital-safety monitoring, including monitoring of pupil screen activity and alerts to the school safeguarding lead when a matter of concern is identified.

- Monitoring is used as part of the school's wider safeguarding arrangements and does not replace professional judgement, staff supervision or the school's safeguarding procedures.
- The school will configure relevant alert categories in line with its risk profile and will review these as risks change.
- Alerts indicating a possible safeguarding concern will be assessed promptly by an appropriately authorised member of staff and escalated to the DSL/Deputy DSL as appropriate.
- High-risk safeguarding concerns will be acted on immediately.
- Monitoring information will be handled confidentially and only accessed by authorised staff for legitimate safeguarding, technical, disciplinary or legal purposes.
- The school will ensure pupils and staff are appropriately informed that monitoring takes place, in accordance with relevant privacy and data-protection requirements.

5.3 Annual filtering and monitoring review

The school will undertake and record a formal review of its filtering and monitoring arrangements at least annually and sooner where significant changes or concerns arise.

The review will involve the DSL, an appropriate member of the Senior Leadership Team, technical/IT support and the governor with relevant digital/online-safety oversight.

The review will consider:

- the effectiveness and coverage of filtering and monitoring;
- pupil risk, including age, vulnerability, SEND and other relevant factors;
- safeguarding incidents, alerts and themes;
- weekly monitoring reports and whether alerts are being acted upon appropriately;
- safe-search settings and access to inappropriate or harmful content;
- AI-generated content and new or emerging online services;
- school-managed devices and any guest/BYOD arrangements, where applicable;
- technical limitations, failures and service-provider updates;
- staff, pupil and parent feedback;
- actions required to improve safety.

The outcome of the review and any actions will be recorded and appropriate assurance will be provided to the governing body.

5.4 Filtering exceptions

If access to a normally blocked website is required for a legitimate educational purpose, staff must obtain appropriate SLT authorisation and follow the school's agreed process with Lancashire Education Digital Services. Requests must have a clear educational reason and must be time limited. Illegal content must not be unblocked.

6. Online-safety education

All pupils receive planned online-safety education through Computing, PSHE and other appropriate curriculum opportunities. Online-safety messages are reinforced through worship, assemblies, newsletters and other school communications.

Teaching is age appropriate and responsive to pupils' experiences and emerging technology. Pupils are taught how to recognise risks, protect themselves and others, report concerns and access help.

The school will use pupil feedback and safeguarding information to adapt its online-safety education.

7. Curriculum content

Online safety is a whole-school responsibility. The curriculum will address, as appropriate to pupils' age and needs:

- online relationships, communication and respectful behaviour;
- cyberbullying and online harassment;
- privacy, personal information, passwords and account security;
- digital footprints and online reputation;
- age restrictions and safe use of games, apps and social media;
- inappropriate or harmful content and how to report it;
- misinformation, disinformation, manipulated content and critical thinking;
- scams, phishing and online financial risks;
- image sharing, consent and digital photography;
- AI, generative AI, deepfakes and responsible use of emerging technology;
- online radicalisation and extremist content in accordance with the school's Prevent responsibilities;

- healthy and balanced use of technology.

Staff will check that online resources are suitable before use and will remind pupils what to do if they encounter inappropriate material. Where pupils undertake independent searches, staff will provide appropriate supervision.

8. Reporting, recording and responding

All staff must report online-safety safeguarding concerns through CPOMS and notify a DSL as soon as possible. The school's Safeguarding and Child Protection Policy sets out the wider reporting, referral, recording and escalation procedures.

Pupils are encouraged to report concerns to a trusted adult and will be taught how to use available reporting, blocking and safety functions.

Where an incident involves potentially illegal content or activity, staff must not investigate beyond what is necessary to ensure immediate safety. The matter must be escalated to the DSL/Headteacher and dealt with in accordance with safeguarding, legal and local procedures.

Incidents will be recorded appropriately and outcomes will be reviewed to identify any learning, support or changes needed to school practice.

9. Digital images and video

Digital images and video can support learning but can also create safeguarding, privacy and reputational risks.

- Staff and pupils will be taught about the risks associated with taking, storing, sharing and publishing images and video.
- Images of pupils must be taken and used in accordance with the school's consent, safeguarding, data-protection and photography arrangements.
- School equipment should be used wherever possible. Any authorised use of personal devices must follow school procedures and images must be transferred/deleted as required.
- The school will maintain an accessible record of pupils for whom photography/publication permissions have been declined.
- Pupils' full names will not normally be published alongside photographs on the school website or other public platforms.
- Once an image or video has been shared online, it can be difficult or impossible to control how widely it is copied, stored or redistributed.

10. Acceptable use

All users must comply with the school's Acceptable Use Policy. Users are expected to use school technology responsibly, safely, legally and respectfully.

Unacceptable use may result in appropriate action under the school's Behaviour Policy, staff disciplinary procedures or other relevant procedures.

Examples of serious or potentially illegal misuse include accessing, creating, sharing or storing child sexual abuse material, extremist or terrorist material, criminally racist material, unlawful adult material or other criminal content or activity.

Where there is an apparent or actual safeguarding or illegal-use concern, the matter must be reported immediately to the Headteacher/DSL/SLT in accordance with the school's safeguarding procedures.

11. Social media

The school recognises that social media can create safeguarding, privacy and reputational risks.

- Staff must not communicate with pupils through personal social-media accounts.
- Professional communication with pupils and families must use school-approved systems.
- Staff must not discuss confidential or personal matters relating to pupils, parents/carers or colleagues on personal social-media platforms.
- Staff should maintain appropriate privacy and security settings on personal accounts and act as positive professional role models.
- Official school social-media accounts must be approved by senior leaders and have clear arrangements for administration, moderation, monitoring and responding to misuse.
- Where possible, at least two authorised staff should have administrative access to official school accounts.
- Any safeguarding concern arising through social media must be reported through the school's safeguarding procedures.

12. Artificial intelligence (AI)

Generative AI tools are increasingly available and may have educational benefits. They can also create safeguarding, privacy, accuracy, copyright, equality and wellbeing risks.

The school will only introduce or permit AI tools for school use where their proposed use is appropriate, risk assessed and consistent with current DfE guidance and the school's data-protection requirements.

- Pupil use of AI will be age appropriate, supervised where necessary and consistent with the supplier's stated age requirements.
- Staff must not enter personal, sensitive or confidential information into AI tools unless the school has specifically authorised the tool and appropriate data-protection safeguards are in place.
- AI-generated information must be checked for accuracy and suitability before being relied upon or shared.
- The school will consider filtering, monitoring, privacy, security and safeguarding implications before introducing learner-facing AI products.
- AI tools used with pupils will be reviewed when significant new features or risks are introduced.
- The school will consider the potential for AI to facilitate bullying, impersonation, manipulation, misinformation or the creation of harmful/deceptive images, audio or video.
- Any AI-generated content used to bully, threaten, humiliate, exploit or otherwise harm a pupil will be treated as a safeguarding concern and reported to the DSL.
- Staff will teach pupils that AI does not replace trusted adults, teachers or real-world relationships and that AI outputs can be inaccurate or misleading.

The school will consider relevant DfE Generative AI Product Safety Standards when assessing AI products for educational use.

13. Data protection and privacy

Online-safety arrangements must comply with the school's data-protection and privacy requirements. Personal data will only be collected, accessed, shared and retained for lawful and appropriate purposes.

- Access to systems and monitoring information will be restricted to authorised users.
- Staff will follow the school's Data Protection/Privacy Policy and relevant information-security procedures.
- Where a new online service or AI product involves high-risk processing of personal data, the school will consider whether a Data Protection Impact Assessment is required.
- Privacy information will be provided in accordance with the school's data-protection arrangements.

14. Staff training and induction

Online safety is part of the school's safeguarding training. Staff will be expected to understand their online-safety responsibilities and know how to report concerns.

- All staff will read the relevant safeguarding information and this policy as part of induction.
- Staff will receive appropriate safeguarding training and updates, including online-safety matters.
- Additional guidance will be provided when significant new risks, systems or technologies are introduced.
- Staff should seek advice from the DSL or appropriate technical lead where they are unsure about an online-safety matter.

15. Monitoring, review and governance

The effectiveness of this policy will be monitored through safeguarding records, filtering and monitoring information, pupil voice, staff feedback, curriculum review, incidents and governor oversight.

The policy will be reviewed at least annually and sooner where there are significant changes to legislation, DfE guidance, Ofsted expectations, technology, school systems or safeguarding risks.

The next scheduled review is September 2027.

16. Related school policies and documents

- Safeguarding and Child Protection Policy
- Acceptable Use Policy
- Behaviour Policy
- Data Protection/Privacy Policy
- Mobile Phone/Smart Technology arrangements
- Computing curriculum / online-safety curriculum
- Cyber-security arrangements
- Staff Code of Conduct
- Complaints and reporting procedures
- Prevent arrangements

17. Current technical service information

Hippings Methodist Primary School's broadband and online services are provided through Lancashire Education Digital Services. The school's service includes Netsweeper web filtering and OnGuard monitoring and alerting.

Current provider/service information, technical documentation and service links should be maintained separately from this policy so that they can be updated without requiring the whole policy to be reissued.

18. Approval

This policy was reviewed in September 2026 and is intended to operate for the 2026–2027 academic year.

Approved by: Governing Body

Date: _____

Chair of Governors: Mrs M Gardner

Signed: _____

Review date: September 2027