Reviewed September 2026
Next Review September 2027

Online Safety and Acceptable Use of the Internet Policy 2026

Technology is an important and essential part of learning at Bewdley Primary School. The school is committed to enabling pupils and staff to use technology confidently, creatively and safely, while recognising that online activity can create safeguarding, wellbeing, data protection and security risks.

This policy sets out how the school provides a safe digital environment, teaches pupils to manage online risk, and establishes clear expectations for the acceptable use of school systems, devices, internet access, communications and emerging technologies.

Aims and scope

This policy aims to:

- safeguard pupils and members of the school community when using technology;
- ensure that online safety is understood as part of the school's wider safeguarding responsibilities;
- provide clear expectations for the safe, responsible and professional use of technology;
- ensure appropriate filtering and monitoring arrangements are in place and reviewed;
- support pupils to become knowledgeable, critical and resilient users of technology;
- set clear expectations for the use of generative artificial intelligence (AI), digital communications, images and online services.

The policy applies to all members of the school community, including teaching and support staff, pupils, governors, volunteers, visitors and contractors who use school technology, school accounts or the school's internet connection. Relevant expectations also apply when school-managed devices are used off site.

Online safeguarding

Online safety is an integral part of safeguarding. Staff must remain alert to the four broad areas of online risk identified in Keeping Children Safe in Education: content, contact, conduct and commerce. Online concerns may include harmful or inappropriate content, grooming and exploitation, cyberbullying, coercion, sexual harassment or abuse, sharing of images, scams, misinformation and disinformation, extremist content, and harmful or inappropriate use of AI-generated content.

Any online concern that may indicate that a child is at risk of harm must be treated as a safeguarding concern and reported immediately in accordance with the school's Safeguarding and Child Protection Policy. Staff should record concerns factually on CPOMS and speak to the Designated Safeguarding Lead (DSL) or a deputy DSL as appropriate.

Roles and responsibilities

Governors

- have strategic responsibility for ensuring appropriate online safety, filtering and monitoring arrangements are in place;
- ensure that filtering and monitoring provision is reviewed at least annually and that actions are recorded;
- receive appropriate assurance about online safety through safeguarding monitoring and the responsible governor.

Headteacher and senior leaders

- ensure this policy is implemented and that staff understand their responsibilities;
- ensure appropriate training and updates are provided;
- work with the DSL, IT support and responsible governor to review filtering and monitoring arrangements;
- ensure serious online safety incidents are managed through the appropriate safeguarding, behaviour, staff conduct or disciplinary procedures.

Designated Safeguarding Lead

- takes lead responsibility for safeguarding and child protection matters identified through online activity or monitoring;
- understands the school's filtering and monitoring arrangements and their safeguarding implications;
- works with senior leaders and IT support to respond promptly to high-risk alerts and emerging risks.

IT support / technical staff

- maintain secure, effective filtering and monitoring systems and provide appropriate technical information to school leaders;
- ensure systems are functioning as intended on relevant school-managed devices and services;
- report safeguarding concerns arising from monitoring to the DSL and maintain appropriate technical records.

Teaching and support staff

- maintain an up-to-date awareness of online safety and follow this policy and the Acceptable Use expectations;
- provide effective in-person supervision when pupils are using connected devices;
- use only approved school systems for professional communication and school information;
- report online safety, filtering or monitoring concerns promptly;
- model safe, responsible and professional use of technology.

Filtering and monitoring

The school will provide appropriate filtering and monitoring systems in line with current Department for Education standards. Filtering is used to reduce access to illegal, inappropriate and potentially harmful content; monitoring is used to identify activity that may require safeguarding, pastoral or technical action.

- Filtering and monitoring will apply, as appropriate, to school-managed devices, school services, users of the school network and guest access.
- Pupil and staff access will be configured appropriately for their roles and needs rather than relying on one blanket profile.
- Filtering must include appropriate protection against illegal content and should take account of text, images, audio, video, apps and AI-generated or dynamic content.
- Monitoring will include appropriate technical monitoring and in-person classroom supervision.
- High-risk safeguarding or malicious activity must be escalated promptly. As a minimum, monitoring arrangements will include weekly reports highlighting incidents and immediate reporting of incidents classed as high-risk.
- Filtering and monitoring provision will be formally reviewed at least once each academic year by senior leadership, the DSL and IT support, involving the responsible governor. The review and resulting actions will be recorded.
- Checks of filtering and monitoring arrangements will be undertaken and recorded at a frequency informed by the school's risk profile.
- Any temporary exception to filtering arrangements must be authorised and documented by the appropriate senior leader.
- Staff must not attempt to bypass filtering, monitoring or security controls. Any site or content believed to be incorrectly blocked or accessible must be reported through the school's agreed route.

Generative artificial intelligence (AI)

Generative AI can support aspects of professional work and learning when used safely and appropriately. Its use must not compromise safeguarding, data protection, confidentiality, intellectual property, curriculum integrity or professional judgement.

- Staff must use school-approved AI tools and services for school business where approval is required.
- Personal, sensitive, confidential or identifiable information about pupils, families, staff or the school must not be entered into generative AI tools unless the tool has been explicitly approved for that purpose and data protection requirements have been satisfied.
- AI-generated material must be checked by a competent member of staff for accuracy, bias, suitability, copyright considerations and age appropriateness before use with pupils.
- AI output must not replace professional judgement, safeguarding decision-making, assessment or accountability.
- Pupil access to generative AI will be age-appropriate, supervised and consistent with the terms of the service and the school's curriculum and safeguarding arrangements.
- The safeguarding implications of AI-generated and personalised content will be considered as part of the school's filtering and monitoring review.
- New AI tools, or materially new uses of existing AI tools, will be appropriately assessed before adoption where their use may create safeguarding, data protection, security or other risks.

Communication technologies and social media

- Professional communication with pupils and parents must take place through approved school systems and accounts. Staff must not use personal mobile numbers, personal email accounts, personal social media accounts or personal messaging services for routine communication with pupils or parents.
- Staff must not use personal email accounts, personal social media accounts or personal messaging services to communicate with pupils.

- Digital communication must remain professional in tone, content and timing.
- Users must not use school systems to bully, harass, threaten, discriminate, impersonate others, share harmful content or undertake unlawful activity.
- Suspected misuse must be reported and managed through the appropriate safeguarding, behaviour, staff conduct or disciplinary route.

Images, video and recordings

- Images and recordings of pupils for school purposes must be captured, stored and shared using school-approved equipment, accounts and systems.
- Staff must not use personal devices to photograph, film or record pupils for school purposes. Legitimate school images and recordings must be captured using school-approved equipment, accounts and systems.
- Images and videos must be handled in accordance with the school's data protection, safeguarding and consent arrangements.
- If a device is believed to contain illegal, sexual, harmful or safeguarding-related material, staff must not routinely view, copy, forward or delete that material. The matter must be referred immediately to the DSL, who will determine the appropriate action.

Personal devices

The detailed expectations for staff, pupils, visitors and volunteers using mobile phones, smartwatches and other personal communication devices are set out in the school's Mobile Phone and Personal Devices Policy. That policy should be read alongside this document.

Online safety education

- Online safety will be taught through Computing, RSHE/PSHE and other relevant curriculum opportunities and revisited regularly.
- Teaching will help pupils recognise unsafe or manipulative content and contact, protect personal information, behave respectfully online, report concerns and critically evaluate online information.
- Teaching will reflect contemporary risks including social media and messaging, image sharing, online exploitation, misinformation and disinformation, scams, persuasive design, AI-generated content and deepfakes where age appropriate.
- Pupils will be taught what to do if they encounter content or communication that worries, frightens or confuses them.
- Where necessary, online safety teaching will be adapted and contextualised for vulnerable pupils, including pupils with SEND, recognising that individual pupils may experience different levels or types of online risk.
- Pupils will receive age-appropriate teaching about cyber security, including password security, scams and phishing, protecting personal information and how to report online or cyber-security concerns.
- Staff will select age-appropriate, current resources, including resources from recognised national online-safety organisations.

Data protection and cyber security

- Users must protect passwords and accounts and must not share login credentials.
- Personal data must be processed only through approved systems and in accordance with the school's Data Protection Policy.
- Users must not deliberately introduce malware, bypass security controls or access another person's account.
- Suspected data breaches, phishing attempts, compromised accounts or cyber-security incidents must be reported promptly through the school's agreed procedures.

School devices used away from school

Staff using school devices away from school must take reasonable steps to keep them secure, including protecting passwords, preventing unauthorised access, not allowing family or friends to use the device, installing required updates and reporting loss, theft or security concerns immediately.

Acceptable Use

Use of the school's digital technology, network, internet access and online services is subject to the expectations set out in this policy. These expectations apply to all pupils, staff and other authorised users; they are conditions of use and do not depend on a separate signed agreement.

All users are expected to use school technology responsibly. In particular, users must not:

- access, create, share or distribute illegal, harmful, abusive, discriminatory or inappropriate content;
- attempt to bypass filtering, monitoring, device management or network security;
- share passwords or use another person's account;
- use school systems for unauthorised commercial, gambling or other inappropriate activity;
- deliberately damage, disrupt or compromise school technology, data or networks;
- use technology in a way that breaches safeguarding, confidentiality, data protection, copyright or professional standards.

Pupils will be taught these expectations in age-appropriate language. Failure to follow them will be addressed through the school's Behaviour Policy and, where appropriate, safeguarding procedures.

Breaches will be considered in context and dealt with proportionately through the school's Safeguarding and Child Protection Policy, Behaviour Policy, Staff Code of Conduct, disciplinary procedures or other relevant procedures. Illegal activity may be referred to external agencies.

Staff training and awareness

All staff, including non-teaching staff, will receive appropriate online safety information and training. Staff will be made aware of the school's filtering and monitoring arrangements, their role in supervising pupils using devices, how to report concerns and the expectations within this policy. Relevant governors will receive appropriate online safety awareness and training.

Parents and carers

The school will support parents and carers to understand online safety risks and school expectations through appropriate communications, guidance and opportunities for awareness raising. Parents should report concerns affecting pupils to the school so that safeguarding or behaviour action can be considered where appropriate.

The school will provide parents and carers with appropriate information about its approach to filtering and monitoring and about significant online platforms or services that pupils are expected to use.

Monitoring and review

This policy will be reviewed at least annually in relation to safeguarding and filtering/monitoring requirements. The review will be supported by an annual online-safety risk assessment that considers and reflects the risks pupils may face online, recognising that technology and associated risks can change rapidly. The policy will be formally reviewed in full by September 2027 or sooner if legislation, statutory guidance, technology, school systems or identified risks change.

Legislation, statutory guidance and related documents

- Keeping Children Safe in Education 2026 (Department for Education)
- Meeting digital and technology standards in schools and colleges - Filtering and monitoring: core standard (DfE, updated 25 August 2026)
- Generative artificial intelligence in education (DfE)

- Generative AI: product safety standards (DfE)
- Data protection in schools (DfE, updated July 2026)
- Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025
- Online Safety Act 2023
- Prevent duty guidance: England and Wales

Related school policies and procedures

- Safeguarding and Child Protection Policy
- Mobile Phone and Personal Devices Policy
- Staff Code of Conduct
- Behaviour Policy
- Anti-Bullying Policy
- Data Protection Policy
- Use of Images / Photography Policy
- RSHE Policy
- SEND Policy
- Educational Visits Policy