



Online Safety Policy

2026-2027

Policy owner	Headteacher / Online Safety Lead
Reviewed by	Mrs H Smith and Ms C Stewart
Review cycle	At least annually and sooner following significant safeguarding, technology or statutory change
Current review	October 2026
Next scheduled review	September 2027
Approval	Governing Body

This policy should be read alongside the school's Child Protection and Safeguarding Policy, Behaviour Policy, Staff Code of Conduct, Data Protection and Privacy arrangements, Acceptable Use Policies and relevant curriculum policies.

1. Purpose and scope

Nateby Primary School recognises that technology is integral to children's learning and everyday lives. Our approach is to enable pupils to benefit from digital technology while safeguarding them from harm and developing the knowledge, behaviours and resilience needed to use technology safely, responsibly, respectfully and securely.

- put the safety and welfare of children first whenever digital technology, the internet, online services, social media or connected devices are used
- give staff, governors, volunteers, pupils, parents and carers clear expectations for safe and responsible technology use
- ensure online safety is embedded within safeguarding, curriculum, behaviour and pastoral practice
- maintain appropriate filtering and monitoring arrangements and respond promptly to concerns
- respond to emerging risks, including generative artificial intelligence (AI), manipulated media, misinformation and disinformation

The policy applies to all staff, governors, volunteers, pupils and other people involved in school activities. Where online behaviour outside school affects a pupil's safety, welfare or the school community, the school will respond through its safeguarding and behaviour procedures as appropriate.

2. Statutory framework and guidance

This policy has been reviewed with regard to current national requirements and guidance, including:

- Keeping Children Safe in Education 2026 (KCSIE)
- Working Together to Safeguard Children
- the current statutory Early Years Foundation Stage framework where applicable
- Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025
- DfE Meeting digital and technology standards in schools and colleges, including the filtering and monitoring core standard
- DfE Teaching online safety in schools guidance

- DfE guidance and resources on the safe and effective use of generative AI in education
- the Prevent duty and relevant safeguarding guidance

The school will update this policy when statutory requirements, technology or the school's risk profile materially change.

3. Understanding online safety risks

Online safety is a safeguarding responsibility. The school considers risks through four broad areas:

Content: being exposed to illegal, inappropriate or harmful material, including misinformation, disinformation, extremist material and harmful or manipulated AI-generated content.

Contact: being subjected to harmful online interaction with other users, including grooming, exploitation, bullying or unwanted contact.

Conduct: personal online behaviour that may increase the likelihood of harm, including unsafe sharing, bullying, misuse of images, privacy breaches and harmful communication.

Commerce: risks such as scams, phishing, inappropriate advertising, in-app purchasing, gambling-style features and other financial exploitation.

Staff remain alert to emerging risks and recognise that technology may facilitate or amplify safeguarding concerns that also occur offline.

4. Roles and responsibilities

Governing Body

- approve and review this policy and seek assurance that online safety arrangements are effective
- hold overall strategic responsibility for ensuring appropriate filtering and monitoring arrangements are in place
- identify a responsible governor for filtering and monitoring and receive assurance about reviews, checks, incidents, trends and actions
- ensure relevant staff receive appropriate training and that online safety is reflected in the school's safeguarding culture

Headteacher and Senior Leadership Team

- maintain oversight of online safety as part of safeguarding and ensure responsibilities are clear
- ensure appropriate filtering and monitoring systems are procured, implemented, reviewed and supported
- ensure significant incidents are managed in line with safeguarding, behaviour, data protection and staff conduct procedures
- ensure decisions about blocked or permitted content and services are proportionate to safeguarding needs and teaching and learning

Designated Safeguarding Lead and Deputy DSL

- take the lead safeguarding role in online safety and work with SLT, the Online Safety Lead and technical support
- review relevant filtering and monitoring reports and respond to safeguarding concerns identified through them
- ensure online safeguarding concerns are recorded and escalated appropriately
- support staff to recognise online safeguarding risks and understand reporting procedures

Online Safety Lead / Champion

- coordinate the day-to-day development and review of online safety practice
- support staff training and curriculum development

- monitor themes and trends from incidents and pupil voice and report relevant information to leaders and governors
- liaise with the DSL and technical support provider

Technical support provider

Nateby Primary School uses an external managed ICT service. The provider has technical responsibility, within the school's agreed arrangements, for maintaining filtering and monitoring systems, security updates and technical controls, providing relevant reports and completing technical actions following concerns or system checks. Technical support works with SLT and the DSL when checks and reviews are undertaken.

All staff and volunteers

- read and follow the Online Safety Policy and relevant Acceptable Use Policy
- use approved school systems professionally for school communications
- supervise and guide pupils' use of technology appropriately
- report online safety, filtering or monitoring concerns promptly using the school's agreed safeguarding procedures
- model safe, responsible and respectful digital behaviour
- protect confidential and personal information and use only approved tools and services for school business

Pupils

- follow the Pupil Acceptable Use Policy and agreed online safety rules
- use technology safely, respectfully and responsibly
- protect passwords and personal information
- tell a trusted adult if something online is worrying, unsafe or inappropriate
- understand that the school may respond to online behaviour outside school where it raises safeguarding or school-community concerns

Parents and carers

Parents and carers are important partners in online safety. The school will provide regular information, including through Weduc, newsletters and relevant awareness resources. Parents and carers are expected to follow school guidance on images, recordings, communication and acceptable use and are encouraged to raise concerns with the school.

5. Filtering and monitoring

The Governing Body has overall strategic responsibility for ensuring appropriate filtering and monitoring. A member of SLT and a responsible governor will oversee assurance that the DfE filtering and monitoring standards are met.

- Filtering is used to reduce access to illegal, inappropriate and potentially harmful content. Monitoring supports the identification of potentially harmful activity and safeguarding concerns.
- The school's filtering is managed with technical support from Ed-it. SurfProtect notifications and reports form part of the school's monitoring arrangements.
- The DSL, SLT and technical support will work together to ensure relevant reports and alerts are reviewed and concerns are acted upon in line with safeguarding procedures.
- Filtering and monitoring provision will be formally reviewed at least once each academic year by SLT, the DSL, technical support and the responsible governor. The review and resulting actions will be recorded.
- Additional reviews or checks will take place following relevant safeguarding concerns, significant changes in working practice, new devices or services, introduction of generative AI tools, major software changes or technical reconfiguration.
- Checks will include school-managed devices, relevant user groups and the effectiveness of filtering. A check log will record when the check took place, who completed it, what was checked and any actions arising.

- Filtering should protect pupils without unreasonably restricting legitimate teaching and learning.
- The school will consider whether its arrangements adequately address real-time, dynamic, personalised and AI-generated content.
- All staff will know how to report concerns about filtering and monitoring and understand that supervision remains important even when technical controls are in place.

6. Artificial intelligence and emerging technology

The school recognises that generative AI can offer educational and administrative opportunities but may also introduce safeguarding, privacy, intellectual property, accuracy and bias risks. AI will therefore be used only where its use is safe, purposeful and consistent with school policies and statutory responsibilities.

- Only school-approved AI tools and services may be used for school business.
- Staff must not enter identifiable pupil information, confidential information or protected pupil work into an AI service unless the school has confirmed that the proposed use has an appropriate lawful basis and the service has been approved for that purpose.
- AI outputs must be checked by an appropriate member of staff for accuracy, bias, suitability and safeguarding concerns before being relied upon or shared.
- Pupil access to AI tools will be age appropriate, planned and supervised, with relevant age restrictions and permissions considered before access is provided.
- Pupils will be taught, at an age-appropriate level, that AI-generated material may be inaccurate, biased, misleading, manipulated or fabricated and that realistic images, audio and video may not be genuine.
- The safeguarding implications of AI, including manipulated media and deepfakes, will be considered within online safety teaching, staff training and filtering and monitoring reviews.
- Safeguarding concerns involving AI-generated content will be managed through the school's safeguarding procedures.

7. Safe use of images, video, mobile phones and personal devices

Images and recordings of pupils are personal data where pupils can be identified. Their use will be consistent with the school's current privacy notices, lawful basis, consent arrangements where consent is relied upon, safeguarding procedures and retention arrangements.

- School-owned equipment should normally be used to photograph or record pupils for school purposes.
- Personal devices must not be used to photograph or record pupils unless an exceptional, specifically authorised arrangement has been approved in advance by the Headteacher and is consistent with safeguarding and data-protection requirements.
- Images and recordings will be transferred and stored only on approved school systems and retained only for the period set out in the school's current retention and privacy arrangements.
- Staff will avoid publishing pupils' full names alongside images unless there is a clear, approved reason to do so.
- Photography and recording in toilet and changing areas are prohibited.
- Parents and carers must follow the school's published arrangements for photography and recording at school events. The school will communicate the applicable arrangements clearly for each event or activity.

Staff use of personal mobile phones during the school day will follow the Staff Code of Conduct and safeguarding procedures. Any exceptional arrangement for trips or residential activities must be agreed in advance by the Headteacher.

8. Communication and social media

- School-related communication with pupils and parents/carers must use approved school accounts and systems.
- Staff must not use personal social-media accounts or personal contact details to communicate with pupils.
- Staff will maintain professional boundaries online and follow the Staff Code of Conduct.

- Pupils will be taught not to disclose personal information unnecessarily, not to arrange unsafe contact, and how to report unwanted or harmful communication.
- Where messaging, collaborative or social technologies are used for learning, they must be school-approved and managed in line with safeguarding and data-protection expectations.

9. Passwords, accounts and information security

- Each authorised user will have an appropriate account and must keep passwords and authentication information secure.
- Passwords must not be routinely shared or kept as class lists. Where younger pupils need account support, staff will use the school's approved account-management or reset process.
- Users must lock or log out of devices when leaving them unattended.
- Pupils must not install unauthorised software or attempt to bypass security, filtering or monitoring controls.
- Any suspected security breach, malware, phishing attempt or loss of information must be reported promptly in line with school procedures.
- School ICT equipment, software and accounts will be maintained and updated through approved technical support arrangements.

10. Online safety education across the curriculum

Online safety is taught through a planned and progressive approach across EYFS, Key Stage 1 and Key Stage 2 and reinforced through Computing, Relationships and Health Education, PSHE and other relevant curriculum areas. Teaching is age and developmentally appropriate and reflects the online experiences pupils may encounter.

Teaching will develop pupils' knowledge and behaviours in areas including:

- using technology safely, responsibly, respectfully and securely
- privacy, personal information, passwords and security
- positive, healthy and respectful online relationships and the effect of online actions on others
- recognising unacceptable behaviour, cyberbullying, grooming, manipulation and harmful contact
- evaluating online information, distinguishing fact from opinion and recognising misinformation, disinformation and persuasive techniques
- online reputation and digital footprints
- copyright, ownership and responsible use of others' work
- online scams, fraud, commercial pressure and age restrictions
- AI literacy, including checking AI-generated information and recognising manipulated or fabricated content
- how, when and where to seek help and report concerns

Online safety is reinforced throughout the year rather than being restricted to a single awareness event.

11. Inclusion, SEND and vulnerable pupils

The school recognises that pupils' online safety needs differ. Teaching, supervision and support will be adapted where necessary to reflect pupils' age, development, communication needs, SEND, EAL and individual safeguarding circumstances. Staff will consider additional vulnerabilities when planning online safety teaching and when reviewing filtering and monitoring provision.

Pupil views will be sought periodically to help leaders understand pupils' experiences, confidence in reporting concerns and emerging online risks. Findings may inform teaching, training and safeguarding actions.

12. Staff, governor and parent awareness

Staff

- Online safety, including filtering and monitoring responsibilities and emerging technology risks, will form part of relevant safeguarding training and updates.
- Staff will receive updates when risks, school systems or procedures materially change.
- Staff will know how to report safeguarding concerns, filtering failures and suspected misuse.

Governors

- Governors will receive appropriate information and training to provide effective oversight of online safety, including filtering and monitoring.
- Relevant reports will include significant themes, trends, review outcomes and actions while respecting confidentiality.

Parents and carers

- The school will share practical online safety guidance through Weduc, newsletters, the school website and other appropriate channels.
- Information will support conversations at home about emerging risks, age restrictions, reporting routes and safe technology use.

13. Responding to incidents and concerns

All online safety concerns must be taken seriously and responded to proportionately. Safeguarding concerns will be recorded on CPOMS and shared with the DSL/DDSL in accordance with the school's safeguarding procedures.

1. Make the pupil or pupils safe and preserve relevant information or evidence where appropriate.
2. Report the concern promptly to the appropriate member of staff. Safeguarding concerns go to the DSL/DDSL; filtering or technical concerns are also referred to the appropriate technical lead/provider.
3. Record safeguarding concerns and actions on CPOMS in accordance with school procedure.
4. Assess whether the concern requires action under safeguarding, behaviour, staff conduct, data protection, Prevent or other procedures and make external referrals where required.
5. Inform parents or carers where appropriate and safe to do so.
6. Review the incident for lessons learned, patterns or changes needed to filtering, monitoring, curriculum, training or policy.

Concerns involving a member of staff or other adult will be managed through the school's safeguarding and allegations/low-level-concerns procedures. Suspected criminal activity or illegal content will be escalated to the appropriate external agency in accordance with safeguarding procedures.

14. Monitoring, review and evidence of effectiveness

The school will review online safety as part of its wider safeguarding cycle. Leaders will consider evidence from:

- CPOMS and online safety incidents, including patterns and trends
- filtering and monitoring reports, alerts, documented checks and the annual review
- pupil, staff and parent/carer views where relevant
- curriculum monitoring and evidence of progression
- staff training and awareness
- new technologies, services and school working practices
- relevant updates to statutory guidance and national standards

Actions arising from review will be recorded and followed up. The policy will be approved by the Governing Body and reviewed at least annually, or sooner where a significant change or incident makes this necessary.

Appendix 1: Filtering and monitoring annual review record

Review item	Record / action
Date and attendees (SLT, DSL, technical support, governor)	
Current filtering and monitoring provision	
Pupil/staff risk profile, including SEND/EAL considerations	
School-managed devices, services and user groups checked	
Generative AI use and ability to address dynamic/AI-generated content	
Filtering check results	
Monitoring reports/alerts and identified trends	
Training or curriculum implications	
Actions, owners and review dates	

Appendix 2: Key related school documents

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection / Privacy Notices and Record Retention arrangements
- Staff, Pupil and Parent/Carer Acceptable Use Policies
- Computing and PSHE / Relationships and Health Education curriculum documentation

Appendix 3: National reference points used for the 2026–27 review

Keeping Children Safe in Education 2026 – Department for Education, September 2026.

Filtering and monitoring: core standard – Department for Education, updated 16 September 2026.

Teaching online safety in schools – Department for Education guidance.

Safe and effective use of AI in education leadership resources – Department for Education, 2026.

State-funded school inspection toolkit – Ofsted, for use on inspections from 7 September 2026.