

Online Safety Policy

September 2026

Nothing is beyond our reach!

Care and challenge engage and motivate us!

Praise reassures and supports us!

Successes are celebrated and built on!

Approved by	Governing Board
Policy owner	Headteacher
Designated Safeguarding Lead	Dawn Joy
Filtering and monitoring lead	Dawn Joy
Date approved	Autumn 2026
Review date	Autumn 2027

This policy reflects Keeping Children Safe in Education 2026 and the Department for Education filtering and monitoring core standard updated in September 2026. It should be read as part of Norton Community Primary School's whole-school safeguarding arrangements.

1. Purpose and aims

At Norton Community Primary School, our vision that 'Nothing is beyond our reach!' includes helping every child become a confident, curious and responsible digital citizen. Technology enriches learning across our Nursery, Reception and Key Stages 1 and 2, but children also need explicit teaching, strong relationships and reliable safeguards so that they can explore the online world safely. Our approach reflects our values of care and challenge: adults provide clear boundaries and protection while helping pupils develop independence, resilience and good judgement.

- Embed online safety as a whole-school safeguarding responsibility, not solely a computing issue.
- Educate pupils about online opportunities, risks, respectful behaviour, privacy, security, misinformation and help-seeking.
- Maintain appropriate filtering, monitoring, cyber security and access controls on school systems and networks.
- Ensure staff understand their online safeguarding responsibilities and know how to respond to concerns.
- Work with parents and carers to support safe and healthy technology use at school and at home.
- Ensure online safety arrangements are inclusive and responsive to pupils with SEND and other vulnerabilities.

2. Statutory and guidance framework

This policy has regard to Keeping Children Safe in Education 2026 (KCSIE), including its requirements and expectations for online safety, filtering and monitoring, staff training and preventative education. It also has regard to the Department for Education digital and technology standards for filtering and monitoring and cyber security, the Prevent duty, statutory Relationships and Health Education guidance, the UK GDPR and Data Protection Act 2018, and relevant safeguarding and communications legislation.

The school's approach to online safety is reflected within its Child Protection and Safeguarding Policy. Online safety is treated as an interrelated theme across safeguarding, curriculum, behaviour, RSHE, staff conduct, data protection, remote education, cyber security and parental engagement.

3. The 4Cs of online risk

Norton uses the 4Cs framework in KCSIE to assess and respond to online risk:

- **Content:** exposure to illegal, inappropriate or harmful content, including pornography, racism, misogyny, self-harm or suicide content, antisemitism, radicalisation and extremism, extreme violence, misinformation, disinformation, fake news and conspiracy theories.
- **Contact:** harmful interaction with other users or generative AI applications that simulate interaction, including peer pressure, grooming, exploitation, inappropriate commercial contact and adults posing as children or young people.
- **Conduct:** online behaviour that causes or increases the likelihood of harm, including cyberbullying and the making, sending, receiving or sharing of sexual or explicit imagery, including AI-generated or digitally manipulated imagery.
- **Commerce:** risks including inappropriate advertising, phishing, scams, financial exploitation, gambling and gambling-like features.

Risk assessment will also take account of emerging technology and behaviours, including generative AI, deepfakes, chatbots, livestreaming, gaming, social media, encrypted messaging, image sharing, location sharing and attempts to bypass school security.

4. Roles and responsibilities

4.1 Governing board

- Ensure online safety is embedded within the whole-school safeguarding approach and relevant policies.
- Ensure appropriate filtering and monitoring systems are in place and receive assurance on their effectiveness.
- Ensure an annual review of online safety and a risk assessment are undertaken, and scrutinise the annual filtering and monitoring review.
- Ensure staff receive appropriate safeguarding and online safety training.
- Ensure cyber security, data protection and information security are appropriately governed and resourced.

4.2 Headteacher and senior leadership team

- Implement this policy and ensure responsibilities are clearly allocated.
- Provide appropriate resources, staff training and technical support.
- Ensure incidents are managed consistently under safeguarding, behaviour, staff conduct and data protection procedures.
- Appoint an SLT member responsible for filtering and monitoring and ensure effective liaison between leadership, the DSL and IT support.

4.3 Designated Safeguarding Lead

The DSL takes lead responsibility for safeguarding and child protection, including online safety, and understands the filtering and monitoring systems and processes in place. The DSL works with the filtering and monitoring lead and IT support to identify risks, review alerts and incidents where appropriate, and ensure online safeguarding concerns are responded to promptly.

4.4 Filtering and monitoring lead / IT support

- Maintain and configure systems in accordance with the school's agreed safeguarding requirements and DfE standards.
- Document filtering and monitoring arrangements, roles, escalation processes and changes.
- Carry out checks and support the annual review, including testing that systems operate as expected on relevant networks, devices and user groups.

- Ensure filtering cannot be readily bypassed and that illegal content is blocked appropriately, while avoiding unreasonable over-blocking that would impede teaching and safeguarding education.
- Escalate safeguarding alerts to the DSL or appropriate safeguarding staff without delay.

4.5 Staff

- Follow the Staff Code of Conduct, Acceptable Use requirements and safeguarding procedures.
- Maintain professional boundaries in electronic communication and use only authorised school systems for school business and communications with pupils.
- Supervise pupils' technology use appropriately and respond to unsafe searches, content or behaviour.
- Report online safety and filtering/monitoring concerns to the DSL or relevant lead promptly, including over-blocking, under-blocking or suspected attempts to circumvent safeguards.
- Never investigate a safeguarding concern in a way that risks further exposure to harmful or illegal material.

4.6 Pupils and parents

Pupils are taught to use school technology responsibly, follow age-appropriate acceptable-use expectations, protect passwords and personal information, respect others and report anything that worries or upsets them. Parents and carers are expected to support Norton's expectations, communicate concerns promptly through the school office, class teacher or Headteacher/DSL as appropriate, and reinforce age-appropriate safe use at home.

5. Curriculum and preventative education

At Norton, pupils are taught how to keep themselves and others safe online through our planned, progressive Computing and RSHE curricula and through everyday teaching across the school. Online safety is revisited in an age-appropriate way from EYFS to Year 6 rather than being confined to an annual event or a single Computing unit. Teaching is age and developmentally appropriate and adapted where necessary for pupils with SEND.

- privacy, personal information, passwords and safe account use
- respectful online relationships, boundaries, kindness and cyberbullying
- recognising unsafe contact, grooming, manipulation, coercion and pressure
- what to do when content or contact causes worry, including how to block, report and seek trusted-adult help
- image sharing and the permanence and potential onward circulation of online material
- critical evaluation of information, misinformation, disinformation, advertising and scams
- age restrictions, healthy technology habits and online wellbeing
- safe and appropriate use and limitations of generative AI and other emerging technologies.

Teaching avoids creating fear and does not expose pupils unnecessarily to harmful material. Pupils are taught that if they experience abuse or exploitation online, it is not their fault and they will be supported when they ask for help.

6. Filtering and monitoring

Norton maintains filtering and monitoring systems appropriate to a primary school's safeguarding risks. Filtering is used to prevent access to illegal, inappropriate and potentially harmful material; monitoring is used to identify potentially harmful activity that may require safeguarding action. These protections apply to school-managed devices and networks as technically appropriate.

The school will identify and document the roles of the governing board, senior leadership, DSL and IT support in filtering and monitoring. Staff will understand the expectations and reporting arrangements relevant to their role.

The school will review its filtering and monitoring provision at least annually and when significant technology, provider, safeguarding or infrastructure changes occur. The review will consider the needs of vulnerable pupils, SEND, emerging risks, generative AI, school-managed devices, relevant personal-device arrangements, system alerts and incidents, and whether filtering is proportionate without unreasonable restrictions on teaching and learning.

The school will test and document filtering and monitoring effectiveness. Concerns about under-blocking, over-blocking, system failure or attempts to bypass controls will be reported to the designated lead/IT support and escalated to the DSL where safeguarding may be involved.

7. Artificial intelligence

Generative AI may be used only where its use is authorised, age-appropriate and compatible with school safeguarding, data protection, curriculum and intellectual property requirements. Staff will assess the safety and suitability of AI tools before pupil use, including whether personal data is collected, what content may be generated, whether interactive features could simulate harmful contact and how filtering and monitoring apply.

Pupils will not be encouraged to enter personal, sensitive or confidential information into unapproved AI tools. AI-generated output will be treated critically rather than assumed to be accurate, unbiased or genuine. Any AI-generated or manipulated image, audio or video used for bullying, sexual harm, impersonation or abuse will be treated as a safeguarding matter.

8. Mobile phones, smart devices and personal technology

As a primary school, Norton operates as a mobile-phone-free environment for pupils throughout the school day, including lessons, assemblies, breaktimes and lunchtimes. Where a pupil brings a phone to school under agreed arrangements, it must remain switched off and stored in accordance with school procedures and must not be accessed during the school day unless an individual exception has been expressly agreed for a specific need.

Smartwatches or other connected devices capable of messaging, recording, photography or internet access must not be used in a way that circumvents the school's mobile-phone or safeguarding arrangements. Staff personal-device use is governed by the Staff Code of Conduct and safeguarding procedures.

9. Images, video and social media

Images and recordings of pupils will be created, stored and shared only for authorised educational or school purposes and in accordance with data protection, consent and safeguarding arrangements. Staff must not use personal devices or personal social-media accounts for unauthorised photographs, recordings or communication with pupils.

The school will not publish information that creates an avoidable safeguarding or privacy risk. Parents attending events will be reminded of appropriate arrangements for photography or sharing where needed. Concerns about pupils' sharing of harmful, sexual or abusive imagery will be handled under the Child Protection and Safeguarding Policy and current national guidance.

10. Responding to online safety incidents

Online incidents may constitute safeguarding concerns even when they take place away from school or on personal devices. Staff must report concerns to the DSL in accordance with safeguarding procedures. The school will take a child-centred response, consider the needs and wishes of affected children, preserve relevant evidence safely where appropriate and involve parents, children's social care, police or other agencies when required.

Where a pupil has accidentally accessed harmful material, staff will respond supportively and avoid blame. Where conduct breaches the Behaviour Policy, proportionate consequences may be used alongside safeguarding and educational responses. Child-on-child abuse will never be dismissed as banter, joking or an inevitable part of growing up.

Illegal material or suspected child sexual abuse material must not be deliberately viewed, copied, printed, forwarded or saved by staff. Staff will immediately seek advice from the DSL and follow safeguarding and law-enforcement reporting procedures.

11. Cyber security, accounts and data

Cyber security is treated as part of safeguarding. The school will work towards and maintain appropriate DfE cyber security standards, including secure account management, appropriate permissions, software and device updates, backups, password security, multi-factor authentication where appropriate, incident response and protection of personal information.

Users must keep passwords confidential, must not attempt to obtain another user's credentials or circumvent controls, and must report suspected compromise promptly. Personal data will be processed in accordance with the UK GDPR, Data Protection Act 2018 and school data-protection policies. Where monitoring involves significant processing of personal data, the school will consider data-protection requirements and a DPIA where appropriate.

12. Remote education and cloud services

Where remote education is provided, the school will use approved platforms and safeguarding arrangements. Staff will maintain professional boundaries, use school-managed accounts, consider privacy and the home environment, and ensure pupils and parents know how to report concerns. Expectations for filtering and monitoring on school-managed devices continue to apply where technically possible outside the school premises.

13. Training

All staff receive safeguarding and child protection training, including online safety and relevant filtering and monitoring responsibilities, at induction. Training is regularly updated, and staff receive online-safety safeguarding updates at least annually and additionally when risks, systems or guidance change.

Staff with specialist responsibilities, including the DSL, filtering and monitoring lead and IT support, receive role-appropriate training so they can interpret alerts, understand system limitations, respond to incidents and contribute effectively to reviews.

14. Working with parents and carers

Norton will use its regular communication with families, including newsletters, website information, parent communications and curriculum information, to share online-safety messages, including age-appropriate services, online relationships, gaming, social media, screen use, scams, harmful content and emerging technologies. Parents will be informed, in appropriate terms, about the school's filtering and monitoring arrangements and how concerns can be reported.

Norton will signpost reliable support such as CEOP Education/Thinkuknow, Childline, Internet Matters and UK Safer Internet Centre resources where useful, while recognising that the school remains responsible for its own safeguarding response.

15. Vulnerable pupils and SEND

The school recognises that some children may be more vulnerable online because of SEND, communication needs, social or emotional needs, previous abuse, care experience or other circumstances. Risk assessment, teaching, supervision and intervention will therefore be personalised where necessary. Accessibility must not mean that essential safeguarding knowledge is omitted.

16. Acceptable use

Norton maintains simple, age-appropriate Acceptable Use expectations for pupils and clear technology-use requirements for staff. These cover responsible use, passwords, privacy, authorised systems, communication, images, copyright, AI, attempts to bypass security, reporting concerns and consequences for misuse. Expectations are communicated and revisited regularly rather than treated as a one-off signature exercise.

17. Annual review, risk assessment and governance assurance

The school will conduct an annual review of its overall online-safety approach, supported by an annual risk assessment reflecting the risks faced by Norton pupils. The review will consider safeguarding incidents, pupil and staff feedback, curriculum coverage, parental engagement, emerging technology, cyber security, filtering and monitoring, vulnerable groups and lessons learned.

The effectiveness of filtering and monitoring will be reviewed at least once each academic year by the responsible SLT member with the support of the DSL and IT support. A record of the review, findings, testing, actions, responsible persons and completion dates will be retained and reported to the governing board.

18. Links with other policies

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Behaviour Policy
- RSHE Policy
- Computing curriculum
- Data Protection Policy and Privacy Notices
- Acceptable Use agreements
- Mobile Phone arrangements
- SEND Policy and SEN Information Report
- Attendance Policy
- Whistleblowing Policy
- Remote Education arrangements
- Cyber Security / IT Disaster Recovery procedures

Appendix 1. Minimum annual online-safety review checklist

- Confirm named SLT filtering and monitoring lead, DSL responsibilities and IT support responsibilities.
- Review the school's online-safety risk assessment, incidents and emerging risks.
- Test filtering on representative pupil/staff accounts, devices and networks and record results.
- Review monitoring coverage, alerts, response times and safeguarding escalation routes.
- Consider AI-generated content, generative AI tools and changes to browsers/apps.
- Check that illegal/harmful content controls and anti-circumvention measures remain effective.
- Check that filtering does not unreasonably restrict required curriculum or safeguarding content.
- Review cyber security, account access and significant data/security incidents.
- Review curriculum coverage, staff training and pupil understanding.
- Consider SEND/vulnerable pupil needs and feedback from pupils, staff and families.
- Record actions, owners, deadlines and report assurance to governors.

Appendix 2. Reporting route

Immediate danger or suspected crime: follow safeguarding procedures and contact emergency/police services where required. Safeguarding concern about a child: report immediately to the DSL or deputy. Filtering/monitoring alert with safeguarding implications: IT/monitoring staff escalate without delay to the DSL. Technical filtering issue without safeguarding implications: report to IT support and filtering/monitoring lead. Data breach or cyber incident: report to the Headteacher/IT lead/Data Protection Officer in line with the school incident procedure. Concern about an adult's online conduct: follow the allegations/low-level concerns and whistleblowing procedures.