GISBURN ROAD C.P. SCHOOL BARNOLDSWICK

ONLINE SAFETY POLICY

DATE AGREED: OCTOBER 2026

REVIEW DATE: OCTOBER 2028

1. Purpose and principles

Gisburn Road Community Primary School is committed to safeguarding and promoting the welfare of every child. Online safety is part of our whole-school safeguarding culture, not a separate technical issue. We want pupils to enjoy the opportunities offered by technology while learning how to use it safely, respectfully, responsibly and confidently.

Our vision is “Where Family and Learning Unite”. Our values of Respect, Kindness, Perseverance, Honesty and Appreciation underpin how we behave online and offline.

This policy aims to:

- protect pupils and adults from online harm, including harmful content, contact and conduct;
- teach pupils how to make safer choices, recognise risks and seek help;
- set clear expectations for use of school devices, networks, online platforms and personal devices;
- set out how filtering and monitoring are managed, reviewed and acted upon;
- ensure concerns are reported promptly, recorded appropriately and managed through safeguarding procedures;
- work in partnership with families, governors, IT support and relevant external agencies.

No filtering or monitoring system can remove every risk. Technology must be supported by effective teaching, appropriate supervision, clear expectations, safe relationships and prompt action when concerns arise.

2. Scope and related policies

This policy applies to school-owned and personal devices when used for school purposes, school networks and accounts, online platforms used by the school, and online incidents outside school where they affect a pupil’s safety, welfare, relationships or behaviour in school.

Read this policy alongside the school’s Safeguarding and Child Protection Policy, Relationships and Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct, Data Protection and Privacy arrangements, Acceptable Use Agreements, and relevant policies for mobile phones, image consent, complaints and staff conduct.

Where an online concern raises a safeguarding issue, the Safeguarding and Child Protection Policy takes precedence. Staff must report concerns to the DSL or a Deputy DSL without delay and record them on CPOMS in line with school procedures.

3. Online risks

The school considers the four broad areas of online risk described in national safeguarding guidance:

Risk area	Examples
Content	Exposure to illegal, harmful, age-inappropriate or misleading material; pornography; violence; extremist content; misinformation; harmful AI-generated content.
Contact	Grooming, coercion, exploitation, unwanted contact, impersonation, scams or contact from adults pretending to be children.

Conduct	Cyberbullying, harassment, discriminatory abuse, sharing images without consent, harmful sexual behaviour, accessing or creating harmful content.
Commerce	Fraud, phishing, in-app purchases, gambling-like features, scams, exploitation of personal or financial information.

Risks may be increased for younger pupils, pupils with SEND, pupils with communication needs, pupils experiencing vulnerability or disadvantage, and pupils who have difficulty recognising or communicating risk. Staff should use age-appropriate, accessible and individualised teaching and support.

4. Roles and responsibilities

4.1 Governing body

- Has strategic responsibility for ensuring appropriate filtering and monitoring systems are in place and that this policy is implemented.
- Appoints a governor to oversee online safety and receives assurance about the effectiveness of arrangements, significant incidents, trends and actions.
- Ensures the annual filtering and monitoring review is completed, recorded and acted upon with Mr Jack Lambert (Primary Technology) and the Designated Safeguarding Lead (DSL), and that the outcome is shared with the Governing Body, in line with the Safeguarding and Child Protection Policy.
- Ensures governors understand their responsibilities and follow the relevant Acceptable Use Agreement.

4.2 Headteacher and senior leadership

- Ensure this policy is communicated, implemented and reviewed.
- Ensure staff receive appropriate training and know how to report concerns.
- Work with the DSL, Mr Jack Lambert (Primary Technology) and the responsible governor to review filtering and monitoring, address identified gaps and ensure the annual review is shared with the Governing Body.
- Approve and document any exceptional, time-limited changes to filtering or monitoring arrangements, following a risk assessment.

4.3 DSL and Deputy DSLs

- Lead the safeguarding response to online safety concerns and ensure they are recorded on CPOMS.
- Review safeguarding alerts and relevant monitoring reports with IT support and ensure urgent concerns are acted on promptly.
- Assess risk, decide on safeguarding referrals and liaise with parents/carers and external agencies as appropriate.
- Ensure online incidents, including cyberbullying, child-on-child abuse and sharing of nudes or semi-nudes, are managed under safeguarding procedures and the relevant national guidance.
- Ensure staff training and pupil education reflect current risks and the needs of pupils.
- Provide the headteacher and governing body with appropriate assurance and anonymised trend information.

4.4 Computing / ICT lead

- Works with the DSL, senior leaders and Primary Technology to ensure technical arrangements support safe learning.
- Reports concerns about devices, accounts, filtering, monitoring or inappropriate content promptly.
- Supports curriculum planning and staff confidence with safe use of technology.

4.5 Primary Technology / IT support

- Maintains technical security, updates, anti-malware protection and agreed filtering and monitoring systems.
- Provides relevant monitoring reports and alerts, including immediate alerts for high-risk incidents and regular reports as agreed.
- Supports technical checks, records system issues and actions, and works with school leaders to resolve gaps.
- Escalates safeguarding concerns identified through technical monitoring to the DSL promptly; IT support does not make safeguarding decisions independently.

4.6 All staff, volunteers, agency staff and contractors

- Read and follow this policy, the Safeguarding and Child Protection Policy, the Staff Code of Conduct and the relevant Acceptable Use Agreement.
- Supervise pupils using devices and model safe, respectful digital behaviour.
- Report concerns immediately to the DSL or a Deputy DSL; do not investigate independently or promise confidentiality.
- Use only approved accounts, platforms and devices for school business and protect passwords and personal data.
- Never use personal devices to photograph, film or record pupils unless a specific authorised exception has been agreed and safeguards are in place.

4.7 Pupils

Pupils are expected to follow the pupil Acceptable Use Agreement, use technology for learning as directed, treat others respectfully, keep personal information private, tell a trusted adult when something online worries them, and never deliberately access, create or share harmful material.

4.8 Parents and carers

Parents and carers are encouraged to discuss online safety with their children, reinforce the school's expectations, report concerns to school and seek advice when needed. The school will share information and resources and will work with families where an online concern affects a child's safety or wellbeing.

4.9 Visitors and other users

Wherever possible, visitors, volunteers and contractors are asked to switch off their mobile phones and lock them away in the lockers at the main office before entering the school. They must follow staff instructions about any device they need to retain. Personal devices must not be used to photograph or record children unless this has been expressly authorised in accordance with school safeguarding procedures. Access to school systems is only permitted where authorised.

5. Filtering and monitoring

The school will maintain appropriate filtering and monitoring arrangements in line with the Department for Education's Filtering and Monitoring: Core Standard and Keeping Children Safe in Education. Netsweeper is the school's current filtering and monitoring tool. The Safeguarding and Child Protection Policy identifies Mr Jack Lambert (Primary Technology) as the school's IT contact for the annual filtering and monitoring review. The DSL and Mr Lambert will review the configuration, monitoring capability, alert arrangements and service effectiveness annually, with the outcome shared with the Governing Body.

5.1 Responsibilities and review

- A documented review of filtering and monitoring will take place at least annually with Mr Jack Lambert (Primary Technology) and the DSL, as required by the Safeguarding and Child Protection Policy. Relevant senior leaders and the responsible governor will contribute as appropriate. The outcome will be shared with the Governing Body. An earlier review will take place if a safeguarding concern, change in technology, major update or change in working practice warrants it.
- The review will consider the school's age range and pupil risk profile, SEND and accessibility needs, school-managed devices, guest access, mobile/app use, any approved AI tools, what is blocked and allowed, monitoring reports, incidents, staff training and curriculum needs.
- The school will record the date, participants, checks completed, findings, decisions, actions, owners and deadlines. The outcome and any actions will be shared with the Governing Body.
- Filtering and monitoring must be active on school-managed devices and school internet access, including guest access where applicable. Any temporary exception must be approved, risk assessed, time-limited and recorded by the authorised senior leader.
- Staff must not bypass or disable filtering or monitoring. If legitimate teaching is blocked, staff should request a review through the agreed school/IT process rather than attempting to circumvent controls.

5.2 Checks and alerts

The school and Mr Jack Lambert (Primary Technology) will agree a documented checking and reporting schedule that meets current DfE expectations. This should include routine checks that systems remain active and correctly configured, regular monitoring reports, and immediate escalation of high-risk safeguarding or technical alerts. The review record will identify when checks occurred, who completed them, what was tested, the outcome and any actions.

The DSL will review relevant alerts and decide the safeguarding response. Technical monitoring supports, but does not replace, staff supervision or the duty to report concerns. Staff must also supervise pupils in person when they are using devices.

5.3 Limitations and safe practice

No system can guarantee that all harmful content will be blocked or all unsafe behaviour detected. Pupils must be taught to stop, close or move away from concerning content and tell an adult. Staff should report any suspected filtering failure or inappropriate access promptly.

The school will consider the risks of real-time, dynamic, personalised and AI-generated content and check whether its current arrangements adequately address them. Any new AI product or significant technology change must be risk assessed before use.

6. Education and prevention

Online safety is taught through the Computing curriculum, Relationships Education, PSHE and other appropriate curriculum areas, assemblies and responsive teaching when risks arise. Learning should be age-appropriate, accessible and sequenced from EYFS to Year 6, drawing on the Education for a Connected World framework and the school's selected online safety resources.

At a minimum, planned discrete online safety teaching will take place at least once each half term, alongside regular reinforcement. The school will maintain a progression overview so coverage is planned and reviewed.

Pupils should learn to:

- keep personal information, passwords and account details secure;
- recognise safe and unsafe content, contact and conduct and know how to report concerns;
- communicate kindly and respectfully, including in games and group chats;
- recognise cyberbullying, discriminatory behaviour, coercion, grooming and manipulation;
- understand consent, privacy and the risks of creating, requesting, saving or sharing images;
- question online information, advertising, scams and AI-generated or manipulated content;
- understand that online actions can affect themselves and others and that harmful behaviour has consequences;
- identify trusted adults and appropriate reporting routes, including how to get help if something has already gone wrong.

Teaching must avoid blaming or shaming children who disclose a concern. Staff should be alert to pupils' age, maturity, communication needs and SEND when responding and planning support.

7. Acceptable use of technology

7.1 School devices, networks and accounts

- School technology must be used for authorised educational or professional purposes and in line with staff instructions.
- Users must not access, download, create, store or share illegal, offensive, discriminatory, sexually explicit, violent or otherwise harmful material.
- Users must not attempt to bypass security, filtering or monitoring, install unauthorised software, access another person's account, or share passwords.
- Pupils may only use websites, apps, cameras, microphones, messaging tools and AI tools with staff permission and supervision.
- Personal data must be handled carefully. Do not upload pupil information, photographs, safeguarding details or confidential school information to unapproved websites, apps or AI services.
- Users must report lost devices, suspected malware, phishing, accidental disclosure, inappropriate pop-ups or possible account compromise promptly.

7.2 Artificial intelligence (AI)

AI tools may create misleading information, imitate people, manipulate images or voices, expose personal information, or generate harmful or sexualised content. Staff must use only school-approved AI tools and follow data protection, copyright, safeguarding and professional conduct requirements. No identifiable

pupil information, confidential school information or safeguarding information may be entered into a public or unapproved AI tool.

Pupils may use AI only when specifically authorised by a teacher and for a clearly defined learning purpose. Staff must teach pupils to check accuracy, question bias, respect intellectual property and understand that AI-generated content may be false or harmful. Any suspected AI-generated or manipulated image of a child, including a 'deepfake' or 'deep nude', must be treated as a safeguarding concern and reported immediately to the DSL.

7.3 Personal devices and mobile phones

Pupil mobile phones and smartwatches are governed by the school's Relationships and Behaviour Policy. Gisburn Road is a mobile phone-free environment. Children in Nursery to Year 4 should not bring mobile phones or smartwatches to school. Children in Years 5 and 6 may bring a mobile phone or smartwatch only for safety reasons when walking to and from school alone. These devices must be switched off before entering the school premises, handed to the class teacher on entry to class and kept in a secured box until home time. Pupils must not access them during lessons, breaktimes, lunchtimes or at any other time during the school day. In exceptional circumstances, including medical monitoring, parents/carers must contact the Headteacher to discuss an individual arrangement.

If a pupil is found using a mobile phone or smartwatch during the school day, or fails to hand it in, the device will be confiscated immediately and stored securely in the school office. Parents/carers will be contacted and asked to collect it. Repeated incidents may result in the pupil losing the privilege of bringing a device to school. Staff must enforce the rules consistently, confiscate devices when necessary and record incidents on CPOMS, in line with the Relationships and Behaviour Policy.

All staff must model appropriate use of mobile phones and must not use personal phones in front of children during the school day. Staff must not use personal phones, cameras, smartwatches or other image-capture devices to photograph, film or record children. School equipment should be used for school purposes. Any exceptional operational need must be authorised in advance and risk-managed in accordance with safeguarding procedures.

In EYFS, mobile phones and personal electronic devices must be stored securely and be inaccessible to children. Personal electronic devices, including smartwatches with image-capturing functionality and smart glasses, must not be used in areas accessed by children, except where authorised in accordance with EYFS requirements and school procedures. Personal devices must not be used during intimate care unless there is a genuine operational reason and the required safeguards and authorisation are in place.

Visitors, volunteers, contractors and parents/carers are asked, wherever possible, to switch off their mobile phones and lock them away in the lockers at the main office before entering the school. Anyone who has a legitimate reason to retain a device must agree this with a member of staff and follow the school's safeguarding instructions. Personal devices must not be used to photograph, record or store images of children unless explicitly authorised in accordance with school procedures. Permission to take photographs at a school event does not automatically permit images to be posted online. The school may restrict photography where needed to protect children's privacy and safety.

7.4 Images, video and consent

- The school will maintain current records of parental/carer permissions and any restrictions and will check these before publishing or sharing identifiable images.

- Use school equipment and approved storage for school photographs and recordings. Do not store pupil images on personal devices or personal cloud accounts.
- Avoid publishing a child's full name alongside their image or other identifying information.
- Ensure children are appropriately dressed and that images are respectful and cannot reasonably be misinterpreted.
- Share images only through approved channels and for a legitimate school purpose. Follow data protection and retention requirements.
- If a parent/carer or child raises a concern about an image, report it to the headteacher or DSL promptly.

8. Reporting and responding to online safety concerns

Any online concern must be reported promptly to the DSL or a Deputy DSL and recorded on CPOMS in line with the Safeguarding and Child Protection Policy. Behaviour incidents, including cyberbullying and misuse of devices, must also be recorded on CPOMS and managed in line with the Relationships and Behaviour Policy and Anti-Bullying Policy, as appropriate. A separate technical log may be used for filtering/monitoring checks, alerts and technical actions, but it must not replace the safeguarding record on CPOMS.

8.1 Immediate steps for staff

1. Listen calmly, take the concern seriously and reassure the child that they have done the right thing by telling an adult.
2. Do not promise secrecy. Explain that information will be shared with the adults who need to help keep them safe.
3. Do not investigate, confront another child, contact alleged perpetrators, or make decisions about referrals independently.
4. Record the child's words as accurately as possible and pass the information to the DSL or Deputy DSL without delay.
5. If a child is at immediate risk of harm, follow the school's safeguarding procedures for urgent referral to children's social care and/or the police.

8.2 Cyberbullying and harmful online behaviour

Reports of cyberbullying, harassment, discriminatory abuse or harmful online conduct will be managed in line with the Anti-Bullying Policy, Relationships and Behaviour Policy and Safeguarding and Child Protection Policy. Staff must report concerns to the DSL or a Deputy DSL without delay and record them on CPOMS. The school will consider the nature and seriousness of the incident, the views and needs of the child affected, any power imbalance, whether there is a pattern, risks to other pupils and any contextual safeguarding concerns.

The school will support the pupil affected, consider proportionate action and interventions for the pupil responsible, contact families when appropriate, and monitor whether the behaviour has stopped. The Anti-Bullying Policy provides for follow-up within four weeks and again during the following half term; this should be applied where relevant. Online incidents outside school may still require school action where they affect safety, wellbeing or behaviour.

8.3 Sharing of nudes or semi-nudes, including AI-generated images

All incidents involving nudes or semi-nudes of children, including digitally manipulated or AI-generated sexualised images, must be reported to the DSL immediately and managed under the current UKCIS guidance and the school's Safeguarding and Child Protection Policy.

- Staff must never view, copy, print, share, store or save the imagery, or ask a child to download or send it to them.
- Do not delete the imagery or ask the child to delete it. Do not ask the child to disclose details about the image; the DSL will decide how to gather information safely.
- Do not blame or shame any child involved. Reassure the child and protect their privacy.
- The DSL will assess risk, consider whether children's social care and/or police must be contacted, decide on appropriate involvement of parents/carers, and record decisions and actions on CPOMS.
- Only in exceptional circumstances, and where necessary to safeguard a child, may the DSL consider viewing an image in accordance with current national guidance and with appropriate safeguards and recording.
- Where an adult is suspected of creating, requesting or sharing sexual imagery of a child, or a child is at immediate risk, urgent referral to police and children's social care must be considered in line with safeguarding procedures.

8.4 Inappropriate content or suspected grooming

If a pupil encounters disturbing or inappropriate content, staff should ensure the pupil is safe, avoid redisplaying the content, note the circumstances without copying the material, and report to the DSL. Suspected grooming, coercion, exploitation, threats, blackmail, extremist content or criminal activity must be escalated immediately. The DSL will determine whether external referrals or specialist support are needed.

8.5 Searching or confiscating devices

Any search or confiscation must comply with the current Department for Education guidance on Searching, Screening and Confiscation, the school's safeguarding procedures and the law. Staff must not assume that the power to confiscate a device gives them an unrestricted right to search it or delete content. Where a device may contain evidence of a crime or safeguarding concern, staff should seek advice from the headteacher/DSL and, where appropriate, the police.

Staff must not inspect or copy nude or semi-nude imagery. In such cases, follow section 8.3 and the current UKCIS guidance. Any decision to search a device must be lawful, necessary, proportionate and undertaken by an authorised member of staff in accordance with current guidance. Decisions, reasons and actions must be recorded.

8.6 Recording and follow-up

Safeguarding concerns and actions must be recorded on CPOMS, including the concern, relevant information, decisions, referrals, contact with families and follow-up. Behaviour incidents must also be recorded on CPOMS in line with the school's behaviour and anti-bullying procedures. Access to records must be limited to those who need the information. Technical logs should record system checks, alerts and technical actions; where an alert raises a safeguarding concern, the DSL must ensure the safeguarding response is recorded on CPOMS.

The DSL will review patterns and trends to inform prevention, pupil support, staff training and governors' oversight. The school will handle complaints through the relevant complaints procedure.

9. Remote learning, social media and communication

- Staff must use school-approved channels for communication with pupils and families. Staff must not communicate with pupils through personal social media accounts or private messaging unless an explicitly authorised and safeguarded arrangement exists.
- Online meetings and remote learning must be planned and supervised appropriately, with clear expectations for conduct, privacy and recording.
- Staff must not post confidential information, pupil images or information that identifies pupils on personal social media.
- Staff must maintain professional boundaries online and report any inappropriate contact, online approach or concern involving a member of staff through the safeguarding procedures.
- Parents/carers should be encouraged to report online concerns directly to school rather than sharing identifiable information about children publicly.

10. Parents, carers and community partnership

The school will raise awareness through communications, the school website, parent information and curriculum events where appropriate. Parents/carers can contact the headteacher or DSL/Deputy DSL about online safety concerns. The school may signpost families to reputable resources including Childnet, UK Safer Internet Centre, Internet Matters, CEOP and Childline.

Where online behaviour affects pupils' safety or relationships, the school will work with families proportionately and sensitively. Information will be shared with parents/carers unless doing so would place a child at risk or compromise a safeguarding response.

11. Staff training and induction

All staff, including temporary staff, volunteers and relevant contractors, must understand the school's reporting routes, acceptable use expectations, filtering and monitoring arrangements, and procedures for responding to online concerns. Online safety is included in induction and safeguarding updates. Training will be refreshed in line with the school's safeguarding training cycle, emerging risks and review findings.

The DSL will identify any additional training needs from incidents, monitoring reports, staff feedback and changes to technology or national guidance.

12. Policy monitoring, review and approval

The Headteacher and DSL will review this policy at least annually, following any significant incident, change to national guidance, introduction of new technology or material change in school systems. The Governing Body will approve the policy and receive assurance on implementation.

The annual review will consider filtering and monitoring effectiveness; incidents and CPOMS trends; pupil, staff and parent feedback; curriculum coverage; training; use of AI and new platforms; mobile phone and smartwatch arrangements; image-capture and visitor arrangements; and whether the policy remains consistent with the Safeguarding and Child Protection Policy, Relationships and Behaviour Policy and Anti-Bullying Policy.

Before approval, the Headteacher/DSL will check the current Netsweeper configuration and operational monitoring arrangements with Mr Jack Lambert (Primary Technology), and will check that the practical arrangements in this policy match the school's procedures and linked policies.

13. Legislation and guidance

This policy should be read with the current versions of the following guidance and legislation. Links should be checked at each annual review:

- Keeping Children Safe in Education 2026 (Department for Education): https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- Filtering and monitoring: core standard (Department for Education, updated 16 September 2026): https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard
- Sharing nudes and semi-nudes: advice for education settings (UKCIS, updated March 2024): https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
- Searching, screening and confiscation (Department for Education): https://www.gov.uk/government/publications/searching-screening-and-confiscation
- Education for a Connected World (UKCIS): https://www.gov.uk/government/publications/education-for-a-connected-world
- Preventing and tackling bullying (Department for Education): https://www.gov.uk/government/publications/preventing-and-tackling-bullying
- Equality Act 2010 and relevant education and safeguarding legislation.

Appendix 1: Pupil Acceptable Use Agreement

At Gisburn Road, we want everyone to use technology safely and kindly. When I use school computers, tablets, the internet or online learning tools, I agree to:

- Use school devices and websites only when my teacher says I can.
- Be kind and respectful online, just as I should be in person.
- Keep my name, address, passwords, school details and other personal information private.
- Use only my own login and keep passwords secret.
- Tell a trusted adult if I see something worrying, upsetting, unkind or inappropriate, or if someone contacts me in a way that makes me uncomfortable.
- Never search for, make, save or share hurtful, rude, violent or sexual material.
- Never take, share or post a picture, video or recording of someone without permission and a teacher's authorisation.
- Never try to get around school safety systems or use another person's account.
- Look after school devices and tell an adult if something goes wrong.
- Remember that anything I post or send may be shared further and can affect other people.

I understand that if I do not follow these rules, an adult will respond in line with the school's behaviour and safeguarding policies. If I am worried about something online, I can tell a trusted adult without fear of being blamed.

Pupil name: _____ Class: _____

Pupil signature (where appropriate): _____ Date: _____

Parent/carer acknowledgement: _____ Date: _____

Appendix 2: Staff Acceptable Use Agreement

All staff, agency staff, volunteers and contractors with access to school technology or pupil information must:

- Use school systems, accounts and approved platforms for professional purposes and in line with this policy.
- Keep passwords secure, use appropriate authentication and lock screens when devices are unattended.
- Never share confidential pupil, family, staff or safeguarding information through unapproved apps, personal email, public AI tools or personal cloud storage.
- Never use personal devices to photograph, film or record pupils unless a specific exception has been authorised in advance and the safeguards have been agreed.
- Use only school-approved AI tools and never enter identifiable pupil data, safeguarding information or confidential school information into unapproved tools.
- Supervise pupils using devices and ensure they use age-appropriate, authorised content.
- Report online safety, cyber security, filtering or monitoring concerns immediately to the DSL or the appropriate technical contact.
- Not investigate safeguarding incidents independently, view or circulate suspected nude/semi-nude imagery, or delete potential evidence.

- Maintain professional boundaries in all online communication and never contact pupils through personal social media accounts.
- Understand that school systems may be filtered and monitored for safeguarding, security and appropriate use, in line with relevant policies and privacy information.

I have read and understood the Online Safety Policy and agree to follow it.

Name: _____ Role: _____

Signature: _____ Date: _____

Appendix 3: Governor, visitor and other user expectations

- Use school internet access and systems only where authorised and for the agreed purpose.
- Do not attempt to access, download or share harmful, illegal or inappropriate material.
- Wherever possible, switch off your mobile phone and lock it away in the lockers at the main office before entering school. Do not photograph, film or record pupils on a personal device unless expressly authorised by the school.
- Do not access or share confidential information unless authorised and necessary for your role.
- Follow staff instructions about phones, devices, photography and online access.
- Report any online safety concern to the headteacher or DSL promptly.

Where appropriate, visitors and other users will be asked to acknowledge these expectations before using school systems.

Appendix 4: Quick reference – responding to an online safety concern

Do	Do not
Listen calmly and reassure the child.	Do not blame, shame or promise secrecy.
Report immediately to the DSL or a Deputy DSL.	Do not investigate independently or confront others.
Record the concern on CPOMS in line with safeguarding procedures.	Do not share details with colleagues who do not need to know.
Preserve the child's safety and privacy; follow DSL instructions.	Do not copy, save, forward or delete suspected nude/semi-nude imagery.
Seek urgent help through safeguarding procedures if a child is at immediate risk.	Do not assume an incident is 'only online' or outside school's remit.

For suspected sharing of nudes or semi-nudes: report immediately to the DSL. Never view, copy, print, share, store or save the imagery, and do not ask a child to download or send it. Follow the current UKCIS guidance.

Appendix 5: Annual filtering and monitoring review record

Complete at least annually with the DSL, relevant senior leader, Primary Technology and responsible governor. Record the outcome and actions.

Review item	Record / evidence / action
Date and participants	
Current filtering provider, products and configuration confirmed	
Monitoring systems and report/alert routes confirmed	
Checks that systems remain active and correctly configured completed	
Student, staff and guest profiles / devices / locations considered	
Coverage of AI-generated, dynamic and app-based content considered	
Current risks, incidents, CPOMS trends and serious alerts reviewed	
Pupil age, SEND, accessibility and risk profile considered	
Staff training and reporting knowledge reviewed	
Curriculum coverage and progression reviewed	
Privacy, data protection and monitoring notices reviewed where applicable	
Actions, owners and deadlines	
Date reported to governing body / committee	
Next review date	

Approval checklist – complete before the policy is adopted

The following are operational checks rather than statements that can be verified from policy wording alone. The headteacher/DSL should confirm these with Primary Technology and the responsible governor before the governing body approves the policy:

- Confirm the current Netsweeper configuration and document the service arrangements and any changes required following the review.
- Confirm the monitoring product(s), alert recipients, frequency of routine reports, immediate high-risk alert route and how the DSL records and closes actions.
- Complete and retain the annual filtering and monitoring review and evidence of checks.
- Confirm that the school's phone, smartwatch, visitor locker and photography arrangements, and EYFS device arrangements, match this policy and the linked safeguarding/behaviour policies.

- Check the availability and current use of any previously named tools, including Whisper and Reputation Alerts; remove references if they are no longer used or supported.
- Check that staff, pupil and governor acceptable-use agreements are issued, signed or acknowledged as appropriate, and stored.
- Check links and policy cross-references, and complete the approval and next-review dates.