



Nicol Mere Primary School

Online Safety Policy

Reviewed September 2026

1. Policy Statement

At Nicol Mere, we recognise that digital technology and the internet are an integral part of children's education, communication and everyday lives. We are committed to ensuring that pupils, staff, governors, volunteers and parents/carers understand how to use technology safely, responsibly and respectfully.

Online safety is an essential part of the school's safeguarding responsibilities. The school will take all reasonable and proportionate steps to protect children from online risks while recognising that no filtering or monitoring system can guarantee that inappropriate or harmful material will never be encountered.

The school will promote a culture in which children feel confident to report anything that makes them feel uncomfortable, worried or unsafe online.

Online safety is the responsibility of everyone within the school community.

This policy should be read alongside the school's:

- Child Protection and Safeguarding Policy
- Acceptable Use Policies
- Behaviour Policy
- Anti-Bullying Policy
- Data Protection and Privacy Policy
- Staff Code of Conduct
- Computing Curriculum
- Relationships, Sex and Health Education (RSHE) Policy
- Complaints Policy
- Mobile Phone/Personal Device Policy
- Remote/Home Learning arrangements
- Cyber Security arrangements

2. Scope

This policy applies to:

- all pupils;
- all members of staff;
- governors;
- volunteers;
- supply and agency staff;
- contractors;
- visitors using school systems;
- parents/carers where they interact with school online systems or social-media platforms.

It applies to technology used:

- on school premises;
- on school-managed devices;

- through school networks and internet connections;
- through school accounts and platforms;
- during educational visits and residential;
- during remote or home learning where school systems are used;
- where online activity outside school has a direct impact on the safety, wellbeing or education of pupils or staff.

3. Aims

The school aims to:

1. Protect children from online harm.
2. Teach pupils to use technology safely, responsibly and respectfully.
3. Develop children's digital literacy, critical thinking and resilience.
4. Provide effective and age-appropriate filtering and monitoring.
5. Ensure that online safeguarding concerns are identified, reported, recorded and acted upon appropriately.
6. Protect personal data and privacy.
7. Ensure staff understand their responsibilities when using technology.
8. Support parents/carers in understanding and managing online risks.
9. Assess new and emerging technologies, including artificial intelligence, before they are introduced.
10. Review online safety arrangements regularly in response to changing technology, emerging risks and statutory guidance.

4. Roles and Responsibilities

4.1 Governing Body

The Governing Body will:

- provide strategic oversight of online safety;
- ensure that appropriate filtering and monitoring arrangements are in place;
- receive appropriate assurance regarding the effectiveness of filtering and monitoring;
- ensure that online safety is appropriately reflected in safeguarding arrangements;
- ensure that the policy is reviewed at least annually;
- ensure that sufficient resources and training are available;
- challenge and support school leaders where appropriate.

4.2 Headteacher

The Headteacher has overall responsibility for ensuring that this policy is implemented effectively.

The Headteacher will:

- ensure that online safety forms part of the school's safeguarding culture;
- ensure appropriate procedures are followed when incidents occur;

- ensure staff receive appropriate training;
- work with the DSL, Online Safety Lead and technical staff to manage online risks.

4.3 Designated Safeguarding Lead

The DSL will:

- have oversight of online safeguarding concerns;
- ensure online safety concerns are managed in accordance with safeguarding procedures;
- ensure concerns are appropriately recorded;
- liaise with external agencies where required;
- ensure staff understand how online concerns should be reported;
- contribute to the annual review of filtering and monitoring;
- ensure emerging online safeguarding risks are communicated to staff and governors.

4.4 Online Safety/Computing Lead

The Online Safety/Computing Lead will:

- coordinate the school's online safety curriculum;
- support staff with online safety education;
- monitor developments in technology and online risks;
- contribute to policy review;
- support staff training;
- work with the DSL and technical support regarding filtering and monitoring.

4.5 IT/Technical Support

The school's technical support/provider will:

- maintain appropriate technical security;
- maintain filtering and monitoring systems;
- ensure security software and systems are appropriately maintained;
- respond to technical incidents;
- support the investigation of online safety incidents where appropriate;
- provide information required for filtering and monitoring reviews;
- escalate significant technical or safeguarding concerns promptly.

4.6 All Staff

All staff are responsible for:

- following the school's Acceptable Use Policy;
- modelling safe and responsible online behaviour;
- supervising pupils appropriately;

- reporting online safety concerns promptly;
- reporting safeguarding concerns directly to the DSL;
- protecting passwords and accounts;
- maintaining professional boundaries online;
- completing required online safety and safeguarding training.

5. Teaching and Learning

Online safety education will be embedded throughout the curriculum rather than being limited to occasional lessons.

It will be taught through appropriate elements of:

- Computing;
- RSHE/PSHE;
- safeguarding education;
- assemblies;
- pastoral provision;
- behaviour education;
- cross-curricular learning.

Teaching will be age-appropriate and progressively developed from EYFS through Key Stage 2.

The school will use an appropriate framework, including the principles within **Education for a Connected World**, to support curriculum planning.

Pupils will be taught about:

- safe and responsible use of technology;
- privacy and personal information;
- passwords and account security;
- appropriate communication;
- cyberbullying;
- online relationships and strangers;
- grooming and exploitation;
- inappropriate and harmful content;
- misinformation and disinformation;
- online reputation;
- sharing photographs and videos;
- gaming and in-app purchases;
- scams and phishing;
- copyright and intellectual property;

- reporting and blocking;
- digital footprints;
- age restrictions;
- artificial intelligence;
- healthy and balanced use of technology.

Pupils will be taught that if something online makes them feel worried, frightened, uncomfortable or confused, they should stop and tell a trusted adult.

6. Online Risk: Content, Contact, Conduct and Commerce

The school recognises four broad areas of online risk.

Content

Children may encounter inappropriate, harmful or illegal material, including:

- violent or disturbing content;
- sexual content;
- extremist material;
- harmful or misleading information;
- inappropriate advertising;
- AI-generated harmful content.

Contact

Children may experience unwanted or harmful contact from others, including:

- strangers;
- grooming;
- manipulation;
- bullying;
- inappropriate messages;
- requests for photographs or personal information.

Conduct

Children may be harmed by their own or others' online behaviour, including:

- cyberbullying;
- abusive messages;
- sharing images without permission;
- impersonation;
- exclusion;
- inappropriate comments;

- harmful challenges;
- damage to reputation.

Commerce

Children may encounter:

- scams;
- phishing;
- inappropriate advertising;
- in-app purchases;
- fraudulent activity;
- gambling-related content;
- pressure to spend money.

The school will incorporate these risks into its teaching and safeguarding arrangements.

7. Acceptable Use

All users of school technology must comply with the relevant Acceptable Use Policy.

Pupils will be taught that school technology must be used:

- safely;
- responsibly;
- respectfully;
- for educational purposes unless otherwise authorised.

Pupils must not:

- deliberately access inappropriate material;
- attempt to bypass filtering or security systems;
- share passwords;
- access another person's account;
- download unauthorised software;
- use technology to bully, threaten or harass others;
- record or photograph others without permission;
- share personal information inappropriately;
- deliberately damage or interfere with school systems.

Misuse will be dealt with in accordance with the school's behaviour, safeguarding and disciplinary procedures.

8. Filtering

The school will provide filtering designed to prevent pupils from accessing inappropriate or harmful online content.

Filtering arrangements will be:

- age appropriate;
- risk assessed;
- regularly reviewed;
- appropriately configured for different user groups where necessary;
- monitored for effectiveness.

The school recognises that filtering cannot guarantee that all inappropriate content will be blocked.

Staff and pupils must report any inappropriate content that is accessible through school systems.

Where inappropriate material is identified, the school will consider:

- whether the material should have been blocked;
- whether filtering settings require adjustment;
- whether the incident represents a safeguarding concern;
- whether the issue should be escalated to the technical provider;
- whether further action or training is required.

9. Monitoring

The school uses appropriate monitoring technology to identify potentially unsafe, inappropriate or harmful activity on school-managed systems. This currently includes **Senso**, where applicable.

Monitoring may include activity such as:

- searches;
- websites visited;
- keywords or phrases;
- inappropriate content;
- safeguarding-related indicators;
- attempts to bypass security or filtering.

Pupils and staff will be informed that use of school systems may be monitored.

Monitoring information will only be accessed by authorised personnel and will be handled in accordance with safeguarding, data-protection and information-security requirements.

Monitoring alerts will be appropriately reviewed and acted upon.

High-risk safeguarding alerts will be escalated immediately to the DSL or appropriate senior leader.

The school will maintain clear procedures identifying:

- who receives monitoring alerts;
- who reviews alerts;
- how alerts are prioritised;
- how safeguarding concerns are escalated;

- how incidents are recorded;
- how technical concerns are reported;
- how monitoring information is retained and securely disposed of.

10. Annual Filtering and Monitoring Review

The school will conduct and record a formal review of its filtering and monitoring provision at least annually and sooner where significant changes occur.

The review will consider:

- effectiveness of filtering;
- effectiveness of monitoring;
- safeguarding incidents;
- blocked and unblocked content;
- false positives and false negatives;
- different user groups;
- school-managed devices;
- remote access where applicable;
- new applications and platforms;
- artificial intelligence tools;
- emerging online risks;
- user feedback;
- technical changes;
- recommendations for improvement.

The review will involve appropriate representatives of school leadership, safeguarding, technical support and governance.

Actions arising from the review will be recorded, assigned to responsible individuals and monitored through to completion.

11. Reporting Online Safety Concerns

Pupils will be encouraged to report concerns without fear of punishment.

A pupil should tell a trusted adult if:

- they see something upsetting;
- someone contacts them inappropriately;
- someone asks for personal information;
- they receive an upsetting message;
- they are bullied online;
- someone asks them to keep an online secret;

- they are asked for a photograph;
- they believe someone may be at risk of harm.

Staff must report safeguarding concerns to the DSL immediately in accordance with the Child Protection and Safeguarding Policy.

Technical or filtering issues should also be reported through the school's agreed technical reporting process.

12. Responding to Online Safety Incidents

When an incident occurs, the school will:

1. Ensure the immediate safety and wellbeing of the child or other person involved.
2. Preserve relevant information where necessary and appropriate.
3. Avoid unnecessary copying, forwarding or viewing of harmful material.
4. Report safeguarding concerns to the DSL.
5. Record the incident appropriately.
6. Consider whether parents/carers or external agencies need to be informed.
7. Consider whether technical or filtering action is required.
8. Review whether further education, support or intervention is necessary.
9. Record the action taken and outcome.

Where there is a concern that a child may be at risk of harm, safeguarding procedures will take priority.

13. Cyberbullying

Cyberbullying will be treated as a safeguarding and/or behaviour matter depending on the circumstances.

The school will:

- investigate concerns;
- support affected pupils;
- take proportionate action against perpetrators;
- involve parents/carers where appropriate;
- provide education and restorative support where appropriate;
- record significant incidents;
- involve the DSL where safeguarding concerns arise.

Online behaviour outside school may be addressed where it affects the safety, wellbeing or education of pupils or staff.

14. Mobile Phones and Personal Devices

Personal mobile phones and other personal devices are not normally permitted for pupil use during the school day.

Where a pupil needs to bring a mobile phone to school for a specific reason, it must be handed to the school office on arrival and collected at the end of the school day, unless an alternative arrangement has been agreed.

Pupils must not use personal devices to:

- photograph or record others without permission;
- access inappropriate content;
- bully or harass others;
- bypass school filtering;
- communicate inappropriately;
- share personal information.

Any agreed exceptions for medical, accessibility or safeguarding reasons will be managed on an individual basis.

15. Social Media

The school recognises that social media presents particular risks for primary-aged children.

Pupils will be taught about:

- age restrictions;
- privacy settings;
- online reputation;
- appropriate communication;
- reporting and blocking;
- risks associated with communicating with strangers;
- the permanence of online content.

The school will not encourage children to create accounts on services where they do not meet the provider's minimum age requirements.

School Social Media

The school's official social-media accounts will be managed only by authorised staff.

Posts will be:

- appropriate;
- professionally written;
- consistent with school policies;
- checked for safeguarding and privacy implications.

Comments and messages will be appropriately moderated.

Personal information about pupils, families or staff will not be disclosed through school social-media accounts.

16. Email and Online Communication

Pupils may only use school-approved email accounts and communication platforms.

Pupils must not:

- share personal information unnecessarily;
- communicate with unknown individuals;

- arrange to meet anyone they have met online;
- send abusive or inappropriate material;
- share another person's information without permission;
- forward inappropriate content.

Pupils must tell a member of staff if they receive an inappropriate or concerning message.

Staff will use school-approved communication systems when communicating with pupils and families.

Staff must maintain professional boundaries and must not use personal accounts for inappropriate communication with pupils.

17. Home Learning and Online Platforms

The school may use platforms including Google Classroom, ClassDojo, video-conferencing tools and other approved educational services to support learning.

Where online learning is provided:

- only approved platforms should be used;
- staff will maintain professional boundaries;
- pupils will be given clear expectations for online behaviour;
- parents/carers will be provided with appropriate guidance;
- live sessions will be appropriately supervised;
- recording will only take place where authorised and necessary;
- personal data will be protected;
- safeguarding concerns will be dealt with through normal safeguarding procedures.

A separate Home Learning/Remote Learning Code of Conduct may provide additional detail.

18. Artificial Intelligence

The school recognises that artificial intelligence, including generative AI, is rapidly developing and may provide educational opportunities as well as safeguarding, privacy, accuracy and ethical risks.

The school will assess AI tools before permitting their use.

Pupils

Pupils may only use AI tools where their use has been authorised by the school or teacher.

Pupils will be taught that:

- AI can produce inaccurate or misleading information;
- AI-generated content should not automatically be treated as fact;
- personal or confidential information must not be entered into AI tools;
- photographs or identifying information about themselves or others must not be uploaded without permission;
- AI should not be used to bully, deceive or impersonate others;
- copyright and intellectual-property rights must be respected;

- AI-generated images, audio and video can be misleading or harmful;
- they must tell an adult if AI produces something upsetting or inappropriate.

Staff

Staff using AI for school purposes must:

- use only approved tools where required;
- follow data-protection requirements;
- not enter confidential, sensitive or unnecessary personal information;
- check the accuracy of AI-generated information;
- consider copyright and intellectual-property issues;
- maintain professional judgement;
- ensure that AI use does not undermine safeguarding or educational assessment.

The school will maintain appropriate guidance for staff and pupils as AI technology develops.

19. Personal Data and Privacy

The school will comply with applicable UK data-protection legislation, including the UK GDPR and Data Protection Act 2018.

Personal information will only be collected, processed, stored and shared where there is an appropriate lawful basis and in accordance with the school's Data Protection and Privacy Policy.

Staff and pupils must not disclose personal information unnecessarily online.

Personal information includes, but is not limited to:

- names;
- addresses;
- telephone numbers;
- email addresses;
- photographs;
- videos;
- usernames;
- passwords;
- location information;
- information about family members.

20. Photographs, Videos and Children's Work

The school recognises that photographs and videos can be an important part of celebrating and communicating children's achievements.

The school will ensure that the collection, storage and use of photographs and videos are managed appropriately.

The school will:

- explain how images may be used;
- obtain and record consent where consent is the lawful basis being relied upon;
- respect withdrawals of consent;
- avoid unnecessary publication of identifying information;
- consider safeguarding circumstances when publishing images;
- use secure systems for storing images;
- restrict access appropriately;
- retain images only for as long as required.

Children's full names will not normally be published alongside photographs on public-facing school websites or social-media accounts.

Children's work will only be published where appropriate permissions and data-protection requirements have been considered.

Parents/carers will be informed of the school's arrangements for photography and filming.

21. Photography at School Events

Parents/carers may be permitted to take photographs or videos at school events subject to the school's instructions.

Parents/carers will be reminded that photographs and videos containing other children should:

- be kept for personal use;
- not be uploaded to public social-media platforms without appropriate consideration of other children's privacy;
- not be copied, distributed or used commercially;
- not be used in a manner that could put a child at risk.

The school may restrict photography or filming where there are safeguarding, privacy or legal reasons to do so.

22. Copyright and Intellectual Property

Pupils and staff will be taught and expected to respect copyright and intellectual-property rights.

Material obtained online must not be copied, downloaded, reproduced or distributed unlawfully.

Where appropriate, pupils will be taught how to:

- identify sources;
- credit creators;
- use copyright-cleared resources;
- understand Creative Commons and other licensing arrangements.

23. Video, Film and Other Media

Any film, video or other media shown to pupils must be age appropriate and suitable for the intended educational purpose.

Teachers must consider:

- age classification;
- content;
- context;
- maturity of the pupils;
- safeguarding considerations.

Where material outside the normal age classification is proposed, appropriate approval must be obtained from the relevant senior leader and, where necessary, parents/carers.

Short extracts will be assessed for suitability rather than relying solely on the classification of the complete film.

24. Passwords and Account Security

Staff and pupils will be taught the importance of keeping accounts secure.

Users must:

- keep passwords confidential;
- not share passwords;
- use strong passwords/passphrases where required;
- log out or lock devices when appropriate;
- report suspected account compromise;
- not attempt to access another person's account.

Staff must not store passwords insecurely or share accounts unless specifically authorised for technical reasons.

25. Cyber Security

The school will maintain appropriate cyber-security measures.

These may include:

- secure network infrastructure;
- anti-malware protection;
- firewalls;
- security updates;
- access controls;
- backups;
- password management;
- appropriate authentication;
- staff awareness training;
- incident response arrangements.

Cyber-security incidents will be reported promptly through the school's agreed procedures.

26. Emerging Technologies

Before new technologies, applications, platforms or devices are introduced for pupil use, the school will consider:

- educational benefit;
- age suitability;
- safeguarding risks;
- data protection;
- privacy;
- terms and conditions;
- minimum age requirements;
- filtering;
- monitoring;
- security;
- accessibility;
- copyright;
- potential inappropriate content;
- AI functionality;
- whether appropriate parental information or consent is required.

The school will not introduce a technology solely because it is popular or freely available.

27. Staff Professional Conduct

Staff must maintain professional boundaries when using digital technology.

Staff must:

- use approved school systems;
- avoid inappropriate online contact with pupils;
- maintain professional communication;
- protect confidential information;
- follow the Staff Code of Conduct;
- report inappropriate contact or online behaviour;
- understand that school systems may be monitored.

Staff must not use personal social-media accounts to communicate directly with pupils unless there is a specific, authorised reason and appropriate safeguards are in place.

28. Staff Training

Online safety training will form part of staff safeguarding and professional development.

Training will include, as appropriate:

- current online risks;

- filtering and monitoring;
- reporting procedures;
- cyberbullying;
- grooming and exploitation;
- harmful content;
- online sexual harassment and harmful sexual behaviour;
- data protection;
- cyber security;
- social media;
- AI;
- appropriate use of technology.

New staff will receive appropriate online safety information as part of induction.

29. Parents and Carers

The school recognises parents/carers as important partners in keeping children safe online.

The school will:

- provide online safety information;
- share appropriate resources;
- signpost parents/carers to reputable advice;
- provide guidance on parental controls where appropriate;
- offer workshops or information sessions where possible;
- communicate significant emerging risks;
- encourage parents/carers to discuss online experiences with their children.

The school will encourage parents/carers to establish appropriate boundaries around:

- screen time;
- online communication;
- gaming;
- social media;
- age restrictions;
- privacy;
- in-app purchases;
- parental controls.

30. Complaints and Concerns

Complaints relating to online safety will be managed in accordance with the school's Complaints Policy.

Where a concern relates to safeguarding, the school's Child Protection and Safeguarding Policy will take precedence.

Concerns about staff online behaviour will be referred to the Headteacher or appropriate senior leader and managed in accordance with the school's safeguarding and staff disciplinary procedures.

31. Monitoring and Evaluation

The effectiveness of this policy will be monitored through:

- safeguarding records;
- online safety incidents;
- filtering and monitoring reports;
- pupil voice;
- staff feedback;
- parent feedback;
- curriculum review;
- staff training;
- technical reviews;
- annual filtering and monitoring review;
- governor oversight.

The school will identify areas for improvement and record appropriate actions.

32. Policy Review

This policy will be reviewed **at least annually** and sooner where necessary following:

- changes to legislation or statutory guidance;
- significant changes in technology;
- changes to filtering or monitoring systems;
- significant online safety incidents;
- changes to school systems or platforms;
- recommendations from safeguarding reviews;
- advice from relevant authorities or professional bodies.

The DSL, Online Safety Lead, Headteacher, technical support and appropriate governor representation will contribute to the review.

Appendix 1 – Online Safety Incident Response

If a pupil encounters something inappropriate online:

STOP → REPORT → RECORD → RESPOND

STOP

Where possible, stop viewing or interacting with the material.

Do not:

- forward it;
- copy it unnecessarily;
- download it;
- share it with other pupils.

REPORT

Tell a trusted adult immediately.

Staff should report safeguarding concerns to the DSL.

RECORD

The incident should be recorded through the school's agreed reporting system where appropriate.

RESPOND

The school will consider:

- safeguarding action;
- support for the pupil;
- parent/carers communication;
- technical action;
- filtering changes;
- monitoring;
- education or intervention;
- referral to external agencies.

Appendix 2 – Useful Resources

The school will signpost staff and parents/carers towards reputable online safety resources, including:

- Department for Education guidance on online safety and safeguarding
- Education for a Connected World
- Childnet
- Internet Matters
- NSPCC Online Safety

- CEOP Safety Centre
- UK Safer Internet Centre
- National Cyber Security Centre

The school will review recommended resources periodically to ensure that links and advice remain current.

This policy will be reviewed annually. The next review date will be September 2027