

Online Safety Policy



Cecil Gowing Infant and Nursery School

Policy owner	Headteacher and Designated Safeguarding Lead
Status and review	September 2026 • Review September 2027
Applies to	Nursery, Reception and Years 1–2; school clubs; staff, governors, visitors and volunteers

Approved by governing board: September 2026 Date: 7th September 2026

Chair of Governors: Julie Bennett

1 Purpose and scope

We help children enjoy and use technology safely. This policy explains how we teach online safety, manage school devices and networks, respond to concerns and work with families. It sits alongside our Safeguarding and Child Protection Policy, Behaviour Policy, Staff Code of Conduct, Data Protection Policy, RSHE curriculum and relevant acceptable use agreements. Safeguarding procedures apply whether a concern arises at school, at home or in a school club.

Our approach reflects Keeping Children Safe in Education 2026, the Early Years Foundation Stage statutory framework, the Department for Education’s filtering and monitoring standard, and the Norfolk Safeguarding Children Partnership procedures. We review the policy at least annually, and sooner if guidance or local risks change.

2 The risks children may encounter

We consider the four areas described in national guidance: content (harmful or misleading material); contact (unsafe interactions with people or conversational technology); conduct (behaviour such as bullying or sharing images); and commerce (advertising, scams, in-app purchases and requests for information). Young children may not have the words to explain what they have seen. Staff respond calmly, listen carefully and take disclosures seriously.

Our values help children practise safe choices: Kindness in how they treat others online; Resilience in asking for help after something upsetting; and Creativity in using technology thoughtfully and safely.

3 Roles and accountability

- The governing board oversees online safety, approves this policy, assures itself that filtering and monitoring are appropriate, and receives a recorded annual review and action plan without identifiable pupil details.
- The headteacher, Mrs Aimee Bradford, is the Designated Safeguarding Lead (DSL). She leads the safeguarding response and understands the school’s filtering and monitoring arrangements. The deputy DSL is Mrs Helen Hoyer. Staff are told how to contact a DSL during school activities and clubs.
- The senior leader responsible for the annual filtering and monitoring review works with the DSL, IT support and the safeguarding governor. Technical IT support maintains controls, provides relevant reports and resolves faults; the DSL decides and records safeguarding action. The school records the assigned role holders in its internal operating records.
- All staff, supply staff, governors and volunteers follow this policy and the safeguarding procedures relevant to their role. They report concerns promptly and do not investigate them themselves.

4 Teaching online safety

Teaching begins in Nursery and Reception through stories, talk, adult modelling, guided use of devices and continuous provision. Children learn that they can stop and tell a trusted adult if something on a screen feels strange, upsetting or unkind. They practise asking before taking a photograph and keeping names and personal details private.

In Years 1 and 2, planned computing and RSHE teaching builds on these foundations. Children learn how to use devices respectfully, recognise that not everything online is true, understand that people online may not be who they say they are, ask before sharing images, and seek adult help with unwanted messages or content. Teaching is revisited through assemblies and ordinary classroom routines. We teach in accessible language and adjust support for children with SEND, communication needs or other vulnerabilities. Pupils are never expected to manage serious online risks alone.

Staff make use of supervised, purposeful screen activities in the EYFS and have regard to current DfE guidance on screen use in early years settings. Technology complements play, movement, conversation and hands-on learning.

5 Safe use of devices and online services

School devices and access

Staff select age-appropriate sites and apps in advance, supervise children's use, and use school-approved accounts and devices for school activities. Children do not access open social media or unsupervised chat as part of school learning. Pupils do not use personal mobile phones during the school day; any exceptional arrangement is agreed by the headteacher and supervised. Staff follow the Staff Code of Conduct on personal devices, photography and communication with pupils and families.

Staff do not use personal accounts to communicate with pupils. Any remote learning or video contact uses school-approved systems, with appropriate privacy settings, supervision and clear information to families about the service and who their child may interact with.

Images, information and artificial intelligence

Staff use school-approved methods to take, store and share children's photographs and work, in line with recorded parental permissions and the school's data protection arrangements. A child's full name is not routinely published with an identifiable image. Images of pupils or their personal information must not be entered into a generative AI tool without an approved purpose, a safeguarding and data protection assessment and appropriate permissions. Pupil-facing AI tools require prior risk assessment and adult supervision; staff check outputs for accuracy and suitability. Any synthetic or altered image used publicly is reviewed for misleading representations and privacy risks.

6 Filtering, monitoring and security

The governing board ensures that suitable filtering and monitoring protect school networks and school-managed devices, including where devices are used away from school if relevant. Filtering blocks harmful and inappropriate material without unnecessarily preventing teaching. Monitoring alerts or reports are reviewed by named staff, escalated to the DSL when they indicate risk and recorded with the action taken. Staff supervision and online safety education remain essential.

At least once each academic year, a senior leader, the DSL and IT support review the arrangements with the responsible governor. They record what systems cover, age and SEND needs, devices and locations, test results, alert routing, incidents, exceptions, provider limitations and actions. Checks are also made after a significant change to devices, software, network settings, working practices or identified safeguarding risk. Any failure is reported promptly to the DSL and IT support; children's access is restricted or supervised differently until the risk is addressed.

Staff protect accounts and pupil data using approved passwords and access controls, report suspected phishing or security incidents promptly, and follow the school's data breach procedure. The technical configuration, named reviewers and alert escalation contacts are held in internal records rather than published on the website.

7 Reporting and responding to concerns

- If a child reports or encounters worrying material, staff reassure them, keep them safe, make a factual record using the school safeguarding system and inform the DSL without delay. They do not promise secrecy, conduct their own investigation, or repeatedly ask the child to recount events.
- If there is immediate danger, call 999. For child protection or immediate safeguarding concerns in Norfolk, the DSL contacts the Children's Advice and Duty Service (CADS) on 0344 800 8021 and follows Norfolk Safeguarding Children Partnership procedures. Staff may make a direct referral if a DSL is unavailable and must then inform the DSL as soon as possible.
- Where an incident concerns harmful sexual behaviour, suspected abuse, exploitation or intimate images of a child, staff do not copy, forward, print or circulate the image. The DSL follows current statutory guidance and seeks police or children's social care advice as appropriate, while supporting every child involved.
- Concerns about the conduct of an adult, including online contact with a pupil or misuse of images, go to the headteacher under the allegations or low-level concerns procedure. If the concern is about the headteacher, it

goes to the chair of governors. The headteacher or chair seeks Local Authority Designated Officer advice when the harm threshold may be met.

The DSL decides how to support the child, whether parents should be informed and whether an external referral is required. If informing a parent could increase risk, the DSL seeks safeguarding advice first. Records are confidential, stored securely and shared only when necessary to safeguard a child. Online bullying or behaviour incidents also follow the Behaviour and Anti-Bullying procedures; safeguarding concerns take priority.

8 Families, training and review

We share age-appropriate online safety advice with parents and carers, including supervision, privacy settings, reporting tools and how to speak with children about what they see. Families can contact the school if something online is affecting their child even when it happened outside school. We explain any online services children are asked to use and the ways school-managed access is protected.

All staff receive online safety and filtering and monitoring information at induction and regular safeguarding updates. The DSL considers patterns from concerns, pupil voice, family feedback and technology checks when planning staff development and curriculum teaching. This policy and the wider online safety risk assessment are reviewed at least annually by leaders and governors.

9 Related guidance and local procedures

Keeping Children Safe in Education 2026: <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

DfE filtering and monitoring core standard: <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard>

EYFS framework and 2026 screen use update: <https://help-for-early-years-providers.education.gov.uk/support-for-practitioners/changes-to-the-eyfs-framework>

Norfolk Safeguarding Children Partnership policies and procedures: <https://norfolkscb.org/about/policies-procedures>

Norfolk Children's Advice and Duty Service: <https://www.schools.norfolk.gov.uk/article/66862/Childrens-Advice-and-Duty-Service-CADS>