



On-Line Safety Policy

Mole Valley Gateway Federation

Newdigate Infant School and St Michael's Infant School

Author	Gayle Priestley (Newdigate Head of School)
Approved by	Nicola Cleather (Federation Head teacher) Governors
Reviewed	October 2025
Review cycle	Reviewed annually, or sooner if required due to changes in statutory guidance.

A Special place to learn and grow

We believe that if we open our hearts and minds to the possibilities, each and every one of us, no matter how small, can achieve and make a difference in our school and beyond.

The parable of the Mustard Seed teaches us that God can do a lot with a little!

1. Introduction

The On-Line Safety Policy is part of the school's Safeguarding Provision Development Plan and links to other policies including Curriculum, Anti-Bullying, Child Protection, and Acceptable Use.

- The On-Line Safety Lead is Gayle Priestley (CEOP trained, Summer 2023).
- This policy has been developed by the school using government guidance and best practice, agreed by staff, and approved by governors.
- The policy and its implementation are reviewed annually.
- This policy complies with Keeping Children Safe in Education (KCSIE 2024/25), the Online Safety Act (2023), the DfE Filtering & Monitoring Standards (2023), GDPR, and the Prevent Duty.

2. Teaching & Learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a statutory requirement in the curriculum and a necessary tool for staff and pupils.
- A wide cross-curricular range of high-quality material can be accessed via the internet to inspire and support children's learning.

Internet use will enhance learning

- The school Internet access includes filtering and firewalls, appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not, with clear objectives for use.
- Pupils learn effective research skills, including knowledge location, retrieval, and evaluation.
- Pupils are shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school ensures compliance with copyright law in the use of internet-derived materials.
- Pupils are taught to be critically aware of online information and how to validate sources.
- Pupils are made aware that images, videos, and text may be generated or altered by Artificial Intelligence (AI).
- Pupils are told to report unpleasant or inappropriate online content to a teacher (in school) or a parent/guardian (at home).

3. Managing Internet Access

Managing filtering

- The school works in partnership with Surrey County Council to ensure filtering systems are reviewed and improved.
- Unsuitable online materials must be reported immediately to the Online Safety Lead and Head Teacher.
- The Chair of Governors, Head Teacher and Online Safety Lead ensure regular checks on the effectiveness of filtering systems.

Information system security

- School ICT systems security is reviewed regularly by Third Sector I.T. and the Safeguarding Lead.
- The school's filtering system blocks access to risky and inappropriate categories in real time.
- Google Safesearch and YouTube Safesearch are enforced, and access to DNS over HTTPS is disabled.
- Activity reports are reviewed weekly to identify risks or breaches.
- Virus protection is updated regularly.

4. Publishing & Parental Guidance

- Contact details on the school website are limited to the school address, email and phone number.
- Staff or pupils' personal details are never published.
- The Head Teacher takes editorial responsibility for ensuring content is accurate and appropriate.
- Parents are reminded that photos or videos of school events (e.g. nativity, sports day, assemblies) must not be shared on social media or other online platforms if they contain images of other children.
- Parents provide written consent on entry to school for the use of photographs for school purposes.

4. E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Staff should avoid opening or sending personal e-mails at school.
- In the Foundation Stage and KS1, e-mails will only be sent and received in a whole-class context.
- If Year 2 pupils participate in individual e-mail correspondence, this will be directly supervised or checked before sending.
- Pupils are taught to report inappropriate e-mails to an adult.
- Pupils are taught never to reveal personal details in e-mails, social media, or online communication.
- Pupils are taught never to arrange to meet anyone online without specific permission.
- Incoming e-mails should be treated with caution; attachments should not be opened unless the sender is known.

5. Publishing Content

School Website

- Only school contact details (address, e-mail, telephone number) will be published.
- Staff or pupils' personal information will not be shared.
- The Head Teacher holds overall editorial responsibility.

Pupil Images and Work

- Pupils' full names will not be used in association with photographs.
- Parents are informed of the image policy in the welcome pack and must give signed consent.

- Parents are reminded that photos or videos of school events (e.g. nativity, sports day, assemblies) must not be shared on social media or other online platforms if they contain images of other children.

6. Social Networking and Personal Publishing

- Access to social networking spaces on the school platform is controlled.
- Pupils are educated in safe use (e.g. passwords, nicknames, avatars).
- Newsgroups are blocked unless approved.
- Pupils must not share personal information or photographs.
- Pupils and parents are reminded that social networking outside school presents risks for primary-aged children.

7. Managing Emerging Technologies

- New technologies are risk-assessed before use in school.
- Pupils are not permitted mobile phones or wearable technologies in school.
- Gaming devices such as Nintendo DS, PlayStation or Xbox are not permitted.

8. Protecting Personal Data

- Personal data will be recorded, processed, and transferred according to UK GDPR and Data Protection Act (2018).
- Staff are trained on secure handling of data and reporting breaches.

9. Policy Decisions

Authorising Internet Access

- All staff must read and sign the Acceptable Use Policy before using school ICT resources.
- Records are maintained of all staff and pupils with access.
- Visitors or community users must also sign an Acceptable Use Agreement.
- Parents sign a consent form for their child's use of ICT.
- Access to the Internet will be by adult demonstration with supervised access to approved on-line materials.

Assessing Risks

- The school takes precautions to prevent access to inappropriate material, though complete prevention cannot be guaranteed. Neither the school nor Surrey County Council can accept liability for the material accessed, or any consequences of Internet access.
- ICT use is regularly audited to assess the effectiveness of the policy.

Handling Complaints

- Complaints about misuse are referred to the Online Safety Lead and Head Teacher.
- Child protection concerns are handled in line with safeguarding procedures.

- Pupils and parents are informed of the school complaints procedure.

10. Communications Policy

Introducing Pupils to the Policy

- Pupils agree to computer rules at the start of each year.
- Pupils are reminded that ICT use is monitored.
- Curriculum opportunities are used to teach online safety throughout the year, with a dedicated Online Safety Week each spring.

Staff and the Policy

- All staff are given the On-Line Safety Policy and its importance is explained.
- Staff are reminded that internet traffic is monitored and traced to individual users.

Parental Engagement

- Parents' attention is drawn to the policy in newsletters, the school brochure and the website.
- Parents are encouraged to attend online safety training sessions.
- Additional information is provided regularly via newsletters and updates linked to Online Safety Week.

11. Monitoring and Review

- The DSL, Head Teacher and Online Safety Lead review implementation annually.
- Governors approve updates and ensure statutory compliance.
- Policy updates reflect new risks, including AI and emerging technologies.