



**Mole Valley Gateway Federation  
C of E Infant School's**  
(Newdigate Infant School and St Michael's Infant School)

## **On-Line Safety Policy**

Author	Gayle Priestley (Newdigate Head of School)
Approved by	Nicola Cleather (Federation Head teacher) Governors
Created	
Review cycle	March 2026

### **Writing and reviewing the On-line Safety policy**

The On-line Safety Policy is part of the School Safe Guarding Provision Development Plan and relates to other policies including the Curriculum Policy, bullying and child protection.

- The On-line Safety leader is Gayle Priestley CEOP trained, Summer 2023.
- Our On-line Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by the teachers and approved by governors.
- The On-line Safety Policy and its implementation will be reviewed annually.
- This policy is in line with Keeping Children Safe in Education

## **Teaching and 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 the pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory 2013 curriculum and a necessary tool for staff and pupils.
- A diverse 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 fire walls, appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

### **Pupils will be taught how to evaluate Internet content**

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be told to report unpleasant Internet content by telling a teacher if in school or a parent/guardian if at home.

## **Managing Internet Access**

### **Managing filtering**

- The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the On-line Safety Leader and the Head Teacher.
- The chair of Governors, Head Teacher and On-line Safety leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- **Information system security**
- School ICT systems security will be reviewed regularly by Third Sector I.T. and the Safe Guarding Lead.
- The school's filtering system blocks access to a range of categories and it updates its databases of risky and inappropriate sites in real time to ensure our network is protected from emerging threats.
- We enforce Google Safesearch, Youtube Safesearch and disable access to DNS over Https as these can be used to bypass filters.
- Activity reports are reviewed on a weekly basis to identify any risks or data breaches.
- Virus protection is updated regularly.

#### **E-mail**

- Pupils and staff may only use approved e-mail accounts on the school system.
- Staff are to avoid opening and sending personal e-mails at school.
- In the Foundation Stage, and KS1 e-mails will only be sent and received in a whole class scenario.
- If Year 2 pupils do participate in individual correspondence by e-mail they will be directly supervised or the e-mail will be checked before being sent.
- Pupils will be taught that if inappropriate e-mails have been received at school or home an adult must be informed.
- Pupils are taught to not reveal personal details, theirs or others, in e-mail/social media/ on-line communication.
- Pupils are taught to never arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

#### **Published content and the school web site**

- The contact details on the Web site are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

#### **Publishing pupil's images and work**

- Pupils' names will be avoided on the Web site, as appropriate, including in blogs, forums, particularly in association with photographs.
- Parents are informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- When children start at the school the parents are given a welcome pack which incorporates a written permission form to be signed and returned before photographs may be shown/published on the school website/in the local newspaper.

## **Social networking and personal publishing on the school learning platform**

- The school will control access to the social networking site on the learning platform, and consider how to educate pupils in their safe use e.g. use of passwords.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must not place personal photos on any social network space provided in the school learning platform.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

## **Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils are not allowed mobile phones or wrist technologies in school.
- Games machines including the Nintendo D.S., Sony PlayStation, Microsoft Xbox and others are not allowed in school.

## **Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

# **Policy Decisions**

## **Authorising Internet access**

- All staff must read and sign the 'Acceptable Use Policy' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Access to the Internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will also be asked to sign an 'acceptable use policy' before being allowed to access the internet.

## **Assessing risks**

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the On-line Safety policy is adequate and that the implementation of the On-line Safety policy is appropriate and effective.

## **Handling On-line Safety complaints**

- Any complaint about staff or children's misuse of the internet must be referred to the On-line safety leader and the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the school's normal complaints procedure.

### **Community use of the Internet**

- All use of the school Internet connection by community and other organisations shall be in accordance with the school On-line Safety policy.

## **Communications Policy**

### **Introducing the On-line Safety policy to pupils**

- Appropriate elements of the On-line Safety policy will be shared with pupils
- At the beginning of every year pupils will agree to the computer rules (Acceptable Use Policy – children)
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of On-line Safety issues and how best to deal with them will be provided for pupils. Every year the school has an on-line safety week. In addition, children are reminded of how to keep safe through-out the year.

### **Staff and the On-line Safety policy**

- All staff will be given the School On-line Safety Policy and its importance explained.
- Staff are made aware that Internet traffic is monitored and traced to the individual user. Discretion and professional conduct are essential.

### **Enlisting parents' support with On-line Safety**

- Parents' and carers attention will be drawn to the School On-line Safety Policy in newsletters, the school brochure and on the school website.
- Parents are encouraged to engage in our On-line Safety training. This may be delivered at school or by video.
- Parents and carers will be provided with additional information on On-line Safety, for example in the school newsletter and in sound bites in the Spring term, which is linked to our On-line safety week.