



# Newport Infant School and Nursery

## Online Safety Policy

Date of Policy Creation/Last Review	October 2022
Policy Lead	Laura Harman, Computing Lead Roisin Whitehouse, Shadow Computing Lead
Date of Policy Adoption by Governing Body	November 2022
Frequency of Review	Annually
Next Review Date	October 2023
Policy Category	Safeguarding

CONTENTS	PAGE NO
Teaching and Learning	3
Communication of the Policy	3
Enlisting Parents' Support	4
Managing Technologies in School	4
Assessing Risk	5
Online Safety Complaints	5
Information System Security	5
Internet Use	5
Personal Data	6
Online Safety Rules Newport Infant School and Nursery Pupils	7
Acceptable Use Agreement Staff, Governor and Visitors Code of Conduct	8

*Newport Infant School and Nursery is committed to safeguarding and promoting the welfare of children. We expect all staff, parents and volunteers to share this commitment.*

- The Online Safety leader in school is Laura Harman, Computing Leader.
- The Online Safety governor is Kerry Dove.
- Our Online Safety policy has been written by the school, building on best practice and government guidance. The document has been agreed by all staff, including senior leaders, and approved by governors.
- This policy applies to all members of the school community (including staff, pupils, volunteers, parents, carers and visitors) and will be renewed every three years.

## **Teaching and Learning**

### ***The importance of internet and digital communications***

- Internet use is part of the statutory curriculum (2014) and a necessary tool for staff and children in the 21<sup>st</sup> century.
- The school has a necessary duty to provide pupils with quality internet access as part of their learning experience.

## **Communication of the Policy**

### ***Introducing the Online Safety Policy to children***

- Key Online Safety messages will be taught and reinforced as part of a planned programme of assemblies, classroom tasks and pastoral activities.
- Pupils will be given clear objectives when using digital devices. They will be taught to recognise acceptable and unacceptable internet use using 'Online Safety Rules'.
- Newport Infant School and Nursery Online Safety Rules will be shared regularly and displayed in every classroom.
- Each half term teachers are expected to deliver an online safety assembly to their class. The contexts are progressive and ensure children are aware of the different elements of digital safety.
- Pupils will understand the need to adopt safe and responsible use of the internet on laptops and mobile devices both in and out of school.
- Pupils are taught to be critically aware of online content and will know how to report unpleasant internet websites or content (CEOP, Report Abuse).
- Pupils will be taught how to publish and present information to a wider audience, whilst respecting the rules of copyright.

## **Staff and the Online Safety Policy**

- All staff will be given the Online Safety policy and its importance explained.

- Teaching staff will receive annual training updates.
- Staff must sign the Acceptable Use Agreement and adhere to these rules at all times.
- Staff should act as good role models in their use of digital devices (see Acceptable Use Agreement).

### ***Enlisting parents' support***

- Specific online safety support is available for parents within the school handbook and on the school website.
- Parents and carers will be drawn to elements of the Online Safety Policy in newsletters.
- Online safety materials will be sent home annually during Online Safety Week to provide parents and carers with advice and support. We also endeavour to send home information each term as a Online Safety Newsletter.

## **Managing Technologies in School**

### ***Mobile Phones***

- With permission of the headteacher, pupils may bring a mobile phone to school where it is seen as a safety precaution. The phone will be handed into the school office at 8:45am and collected at the end of the day.
- The sending of abusive or inappropriate messages is forbidden and will be dealt with in accordance with our anti-bullying policy.
- Staff should always use the school phone to contact parents, unless the use of own mobile phones is agreed by the headteacher.
- Staff and volunteers are only permitted to use mobile phones in the staff room during breaks.
- Parents are regularly informed that the use of mobile phones is **not** permitted on the school site. An exception is made during pupil performances, as described below.

### ***Photographs/Video Recording***

- Staff should use a school camera to capture images, rather than their personal devices.
- Photos taken by the school are subject to the Data Protection Act.
- Pupils will not be permitted to use cameras unless specifically authorised by a staff member.
- Parents/carers are permitted to photograph/record their own child in pupil performances, but they must not publish content online if it contains images of other children. The headteacher or deputy headteacher will inform parents of this at every public event.
- Parents must not use mobile phones on school visits to take pictures of pupils.

### ***Published Content and the School Website***

- Contact details for the school may be viewed on the school website ([www.newportinfants.co.uk](http://www.newportinfants.co.uk)). This will consist of the telephone number, address, email address and senior staff details.
- Personal information of staff and pupils will not be published.
- The Headteacher and Computing Leader will ensure that content on the school website is accurate, appropriate and up to date.

- Consent from parents will be obtained before photographs or videos are uploaded to the school website.

### **Assessing Risk**

- The school will audit ICT use to establish if the Online Safety Policy is adequate, appropriate and effective in practice.
- As a staff we will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale, it is not possible to guarantee that unsuitable material will never appear on a school device. The school does not accept liability for the material accessed, or any consequences of internet access. We do, however, report any inappropriate content to CEOP immediately.

### **Online Safety Complaints**

- All safeguarding concerns, including online safety issues, may be reported to the Designated Safeguarding Leads in school: Mrs C Pierce, Mrs E Heeley, Miss E Russell or Miss E Harrow. These incidents are dealt with in line with the school's safeguarding policy.
- Incidents are recorded on CPOMS and external agencies are informed if necessary.
- Complaints of internet misuse, including staff misuse, will be dealt with by the head teacher, Mrs Chris Pierce.
- Discussions will be held with community police if handling potentially illegal issues.

### **Information System Security**

- The school's ICT system security is provided by Telford and Wrekin and will be reviewed regularly. Virus protection and filtering will be updated when necessary by our school ICT Consultant, Shaun Watkins. Security strategies will be discussed with the Local Authority.
- A security breach, lost/stolen equipment, virus notifications or unsolicited emails must be reported to senior management.

### **Internet Use**

#### **School Use**

- Pupils will regularly access safe materials via the internet in school.
- Staff will review all content before pupils access websites or online learning platforms.
- The school will seek to ensure that the use of internet derived materials complies with copyright law.

#### **Home Use**

- Our pupils are under the age of 13 and therefore considered too young to hold a social media account, but we recognise that they may have access to these sites at home. We regularly issue pupils with information to stay safe online and ask parents to supervise and ensure their security levels are high on home devices.
- Pupils are discouraged to search for raw images online. If internet research is set as a home learning task, suggested websites will be included.

### **Password Security**

- Pupils are taught to acknowledge that passwords are private and not to be shared.

- Staff are regularly reminded to ensure their passwords are individual and not to be shared with others.

### **Online Communications**

- Pupils are introduced to email as part of the Computing curriculum.
- Pupils are taught to immediately inform an adult if they receive an inappropriate or offensive message or email (through their Purple Mash account).
- Staff to pupil online communication must only take place via a learning platform (e.g. Purple Mash or Class Dojo).
- Staff are permitted to access email via a school approved account on the school system.

### **Personal Data**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and Freedom of Information Act.

# Newport Infant School

## Online Safety Rules

### Be kind

Always be polite and treat people kindly online, just like in real life.



### Keep passwords private

Don't share your password with friends or strangers.



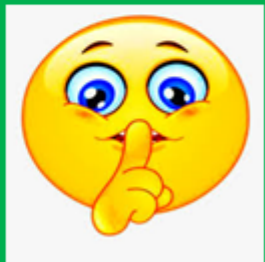
### Tell a grownup

Always tell a trusted adult if you see something online that upsets you.



### Don't share personal information

Use an avatar profile picture where possible and don't share your real name, address or school.



*I am responsible for my own behaviour online.*

*I know that these rules keep me safe.*

### **Acceptable Use Agreement: Staff, Governor and Visitors**

**By signing this agreement, you will have access to the school's systems and acknowledge that you agree to all the statements below. Additionally, that you have read and understand school policies which have a bearing on this agreement.**

- I will educate the children in my care about the safe use of digital technologies, acting on any online safety concerns in accordance with the school's policies.
- I understand my use of the school's ICT systems/networks and internet is monitored.
- I recognise that whether within school or out of school, I must abide by the statements set out in this document when using systems that relate to the school or impact on my role within the school and wider community.
- I know what GDPR is and how this has a bearing on how I access, share, store and create data.
- Any data that I have access to away from school premises must be kept secure.
- As outlined in the school's data protection policy, it is my responsibility to ensure when accessing data remotely that I take every bit of reasonable care to ensure the security of the data is maintained.
- I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content can have a bearing on my professional role.
- I will not give out my personal details, such as a mobile phone number, personal email address or personal social media account to pupils or parents.
- I recognise that my social media activity can have a damaging impact on the school and children in my care if I fail to uphold my professional integrity at all times whilst using it.
- If I am contributing to the school's social media account or website I will follow all guidelines given to me, with particular care given to what images/videos and details can be uploaded.
- I will never upload images/videos of staff/pupils or other stakeholders to my personal social media accounts unless there is significant reason to and permission has been granted by the headteacher in writing for each occurrence.
- I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others' behaviour/conduct, I will notify the school at the earliest opportunity.
- I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others.
- I will never download or install software unless permission has been given by the headteacher Chris Pierce.
- I shall keep all usernames and passwords safe and never share them.
- I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/ services/content remotely.
- Any personal devices I own shall not be used to access school systems/data/services/content remotely unless I have adequate virus protection and permission from the school.
- I understand that mobile devices, including smart watches, shall not be used, nor in my possession, during times of contact with children.
- Any school trips/outings or activities that require a camera will be provided by the school and any data collected on them will be used in accordance with school policies.
- At no point will I use my own devices for capturing images/ video or making contact with parents/carers unless this is agreed by the headteacher Chris Pierce.

**I agree to follow and adhere to these e-Safety rules and will support the school's approach to online safety.**

**Signed \_\_\_\_\_ Date \_\_\_\_\_**