



## 1.12 NURSERY ONLINE SAFETY POLICY

This policy outlines how Brockham Green Nursery ensures the safe, responsible, and age appropriate use of digital technology for all children in our care. It forms part of our wider safeguarding arrangements and supports the Early Years Foundation Stage (EYFS) statutory framework.

### **Our Aims**

- To protect children from online risks, including harmful content, contact, and conduct.
- To promote supervised, age appropriate digital learning experiences.
- To guide staff in the safe use of technology.
- To work with parents to support consistent online-safety messages at home and Nursery.

### **Roles and Responsibilities**

#### Designated Safeguarding Lead (DSL)

- Leads on all online safety matters.
- Ensures procedures align with safeguarding policies, UKCIS guidance, and statutory Requirements.
- Provides staff with training and updates.
- Responds to online safety incidents or concerns.

#### Nursery Staff

Supervise children at all times when using digital devices.  
Ensure all digital resources are safe and age appropriate.  
Model positive, responsible technology use.  
Report any concerns immediately to the DSL.

#### Parents/Carers

- Work in partnership with the Nursery to promote safe online habits.
- Ensure photos or videos taken on Nursery premises do not include other child unless permission is given.
- Use only official Nursery communication channels.

### **Children's Use of Digital Technology**

Digital technology is used to support early learning (e.g.-phonics, counting, creative apps) record observations of children's development.

#### Children

Use tablets or interactive boards only under direct adult supervision.

Access apps or websites pre-approved by Nursery staff.

Do not use messaging, chat, video calling, or social media platforms.

Are encouraged to tell a trusted adult if they see something confusing or upsetting

It is very important to us that digital use within Brockham Green Nursery is limited and balanced with outdoor play, hands on learning, and social interaction

### **Staff Use of Technology**

Staff **MAY NOT** use personal devices (phones/tablets) to take photos or videos of children.

Staff mobile phones must be stored in the designated staff area during sessions.

Only Nursery devices are used for educational activities or capturing observations.

Staff follow data protection and confidentiality requirements when handling digital information

### **Internet Safety, Filtering, and Monitoring**

All Nursery devices connected to the internet use filtering to block inappropriate content.

Staff immediately report any accidental exposure to unsuitable content

All digital resources are reviewed regularly for suitability and safety.

### **Teaching Children about Online Safety**

- Online safety is introduced in simple, meaningful ways using story books and puppets for Example
- Circle time discussions about trusted adults
- Games or role play to help children understand i.e.
  - You don't talk to strangers online
  - You ask an adult before using a device
  - You tell an adult if something doesn't feel right

The goal is not to overwhelm children, but to help them build awareness and confidence.

### **Use of Images, Videos, and Children's Work**

Parental consent is obtained before photographing or filming children.

Images are stored securely on Nursery devices and used only for educational or Assessment purposes (eg-Tapestry or similar platforms)

Photos will not be shared on personal devices or personal social media accounts.

Parents are reminded not to upload photos of other children to social media.

### **Communication With Families**

The Nursery communicates through official channels such as newsletters, emails, secure Parent apps, and noticeboards.

Staff do not use personal social media to contact parents.

The Nursery may share personnel achievements or events on official platforms with parental consent.

### **Data Protection and Privacy**

- All digital data is stored securely in line with UK GDPR requirements.

- Only authorised staff have access to digital records.
- Passwords, login details, and assessments platforms are protected.
- Devices are locked when not in use.

### Responding to Online Safety Concerns

Any concerns about harmful content, inappropriate behaviour, or online risks must be reported to the DSL immediately

The DSL will.

- Log the concern.
- Investigate in line with safeguarding procedures.
- Inform parents where appropriate.
- Refer to external agencies (eg- LADO, police, children's services) if necessary.

### Staff Training

- All staff receive online safety and digital safeguarding training as part of induction.
- Training is refreshed regularly and whenever guidance changes

Date reviewed – November 2025