**Online Safety Policy**

**Introduction**  
It is essential that children are taught to use technology safely and are equipped to manage the risks posed in both the physical and digital worlds. This policy applies to all devices with internet capabilities and addresses potential risks:

* **Content**: Exposure to illegal, inappropriate, or harmful material.
* **Contact**: Harmful online interactions with others.
* **Conduct**: Behaviour that causes or increases the likelihood of harm.

**ICT Equipment**

* Tablets are used solely for observation, assessment, planning, and taking photographs for children’s learning journeys.
* Tablets remain on the premises and are stored securely when not in use.
* Staff adhere to the guidelines provided for using these systems.

**Internet Access**

* Children are never left unsupervised while using the internet.
* Only reputable, child-friendly websites (e.g., CBeebies) are accessed.
* Video-sharing sites like YouTube are used only when staff pre-screen content.

**Children are taught online safety principles in an age-appropriate way:**

* Go online only with a trusted adult.
* Be kind and keep personal information private.
* Click only on things they understand.
* Tell an adult if something online makes them upset.

Staff support children’s resilience by teaching safety, appropriate friendships, seeking help, and understanding that secrets should not be kept when unsafe.

**Personal Mobile Phones and Internet-Enabled Devices**

* Staff and visitors must not use personal mobile phones during working hours, except during breaks and in designated areas away from children (office).
* Phones are stored in a designated secure area (office).
* Staff must ensure the setting’s contact details are shared with anyone needing to reach them during work hours.
* Mobile phones are not taken on outings, and staff must not use personal devices to photograph or record children.
* Parents and visitors are prohibited from using mobile phones on the premises, except in designated private spaces.

**Cameras and Video Recordings**

* Staff must not bring personal cameras or video equipment to the setting.
* Photographs and recordings are taken only for valid purposes, such as documenting learning or creating displays, and only with setting-owned equipment.
* The setting manager monitors the use of cameras and videos.
* Parents must obtain permission to photograph or record children during events. They are reminded not to share or upload images of other children.
* Photographs for publicity purposes require parental consent and measures to minimize safeguarding risks.

**Cyberbullying**

If staff become aware that a child is a victim of cyberbullying, they:

* Discuss the issue with the parents and provide guidance.
* Refer parents to appropriate resources, such as:
  + **NSPCC**: 0808 800 5000, [www.nspcc.org.uk](https://www.nspcc.org.uk)
  + **ChildLine**: 0800 1111, [www.childline.org.uk](https://www.childline.org.uk)

**Social Media Use**

We only post images of children on social media platforms with **prior written permission** from their parents or guardians.

* Consent is obtained during the registration process or via specific requests for events or activities.
* Images shared on social media are carefully selected to protect children’s identity, and personal details (e.g., names) are not included.
* Parents and guardians are welcome to withdraw their consent at any time.

**Staff must**:

* Avoid discussing or naming the setting online.
* Consider the permanence and accessibility of any online comments or images.
* Maintain confidentiality and refrain from discussing work-related issues.
* Use good judgment when posting content and ensure it cannot harm the setting or relationships with families.
* Restrict social media connections with parents or children unless pre-existing personal relationships are disclosed and managed through a risk assessment.

Any concerns or breaches must be reported to the designated safeguarding lead.

**Inappropriate Images and Online Grooming**

* Staff understand that distributing indecent images is illegal, and online grooming is a serious offence.
* Any concerns about a colleague’s behaviour must be reported to the designated safeguarding lead.

**Implementation and Monitoring**  
The setting manager ensure staff have access to resources and training to support safe and effective use of technology. This policy is regularly reviewed to ensure compliance and relevance to evolving technologies.