



## **E-Safety Policy**

### **Policy statement**

All staff at Tiggers have a duty to ensure children are protected from potential harm resulting from online technologies within the setting. Staff must make every effort to safeguard against all risks, ensuring a safe and secure environment for children.

### **Staff Responsibilities**

- Ensuring the policy is implemented and compliance is actively monitored.
- Reporting procedures and requirements should an incident occur.
- Ensuring an E-Safety incident log is appropriately maintained and reviewed.
- Keeping up to date with E-Safety issues and guidance.

### **Use of Social Networking Sites**

- To maintain professional distance and avoid unwanted contact, staff must not link their personal social networking accounts to the nursery website.
- Staff must not contact children's parents or family members on social networking sites.
- Privacy settings should be set to the highest levels and checked regularly.
- For safeguarding purposes, photographs or videos of children must not be shared on social networking sites.

### **Personal mobile devices**

- Staff must hand in personal mobile devices into the office at the beginning of each day. Under no circumstances does Tiggers allow a member of staff to use their device whilst working.
- Personal mobile devices include smart watches – these must be disabled for text message, data and call connectivity.
- Users bringing in personal devices must ensure there is no inappropriate or illegal content on the device.
- Tiggers is not responsible for the loss, damage or theft or any personal mobile device.

### **Photographs and Videos**

- As photographs and videos of children are regarded as personal data in terms of the General Data Protection Regulation, GDPR (2018) we must have written permission for their use from parents/carers.
- Parental consent for use is obtained annually.
- Only authorised nursery equipment may be used to take photographs or videos of children for nursery purposes. The use of personal videos and cameras is not permitted in nursery.

- When taking photographs/videos staff must ensure children are appropriately dressed and not participating in activities which could be misinterpreted.

### Storage of Images

- Images are stored only on nursery equipment and do not leave the premises.
- Staff must not remove images from nursery equipment with portable media storage devices.
- Rights of access to images are restricted to teaching staff and the confines of the nursery.

### Laptops

- Staff must be aware that nursery laptops are subject to monitoring in accordance with E-Safety policies. All activities carried out on setting devices are open to scrutiny.
- Laptops should be made available for anti-virus updates, software installations or upgrades.
- Setting devices must only be used for professional purposes and, if containing sensitive information or photographs, should not leave the premises.

### Children's use:

- Children are not permitted to access the internet or use the setting's staff laptops at any time. Children are permitted access to authorised children's ICT toys, which do not have access to the internet.

### Data Storage and Security

- In line with the requirements of the General Data Protection Regulation, GDPR (2018), sensitive or personal data is recorded, processed, transferred and made available to management in the nursery. This data must be accurate, secure and lawfully processed; processed for limited purposes and in accordance with the data subjects rights; adequate, relevant and not excessive; kept no longer than necessary and only transferred to others with adequate protection.

### Serious Incidents

- If a serious incident occurs, such as inappropriate content is accessed, an E-Safety incident log is made and a nominated officer is informed.

This policy was adopted at a meeting of	Tiggers Nursery	<i>(name of provider)</i>
Held on	01 September 2023	<i>(date)</i>
Date to be reviewed	01 September 2024	<i>(date)</i>
Signed on behalf of the provider		
Name of signatory	Andrew Pitayanukul	
Role of signatory (e.g. chair, director or owner)	Director	

### E-Safety Incident log

Details of all E-Safety incidents to be recorded by staff and monitored.

<b>Date of incident</b>	<b>Name of individual involved</b>	<b>Device number</b>	<b>Details of incident</b>	<b>Actions and reasons</b>	<b>Confirmed by</b>