E-safety (including all electronic devices with imaging and sharing capabilities)

Online Safety

It is important that children and young people receive consistent messages about the safe use of technology and are able to recognise and manage the risks posed in both the real and the virtual world. Terms such as 'e-safety', 'online', 'communication technologies' and 'digital technologies' refer to fixed and mobile technologies that adults and children may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks. The issues are:

Content – being exposed to illegal, inappropriate or harmful material

Contact – being subjected to harmful online interaction with other users

Conduct – personal online behaviour that increases the likelihood of, or causes, harm

I.C.T Equipment

- All computers have up-to-date virus protection installed.
- Tablets are only used for the purposes of observation, assessment and planning and to take photographs for individual children's learning journeys.
- Tablets remain on the premises and are stored securely at all times when not in use.
- Staff follow the additional guidance provided with the system
- Screen based assistive technologies may be used to support staff or children in the setting on a case by case basis
- Families are informed of how the setting is supporting children's use of technology.

Content

- Children should not be alone when using devices. Screen time should be with the co-engagement of an adult
- Screen time for children 2-5 years should be limited to less than one hour per day – this includes time spent on screens at home.
- Any content should be slow, repetitive and predictable to support children's learning. It should be free of adverts, scrolling and autoplay features.

- Staff should use their professional judgement when assessing educational tools, software and apps.

Internet access

- Children never have unsupervised access to the internet.
- Only reputable sites with a focus on early learning are used – e.g. CBeebies, Super sounds, Cosmic Yoga and Tapestry
- Children are taught the following stay safe principles in an age appropriate way:
  - only go online with a grown up
  - be kind online **and** keep information about me safely
  - only press buttons on the internet to things I understand
  - tell a grown up if something makes me unhappy on the internet
- Staff support children's resilience in relation to issues they may face online, and address issues such as staying safe, appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
- All computers for use by children are sited in an area clearly visible to staff.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.

The setting manager ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

Strategies to minimise risk include:

- Check apps, websites and search results before using them with children.
- Children in Early Years should always be supervised when accessing the internet.
- Ensure safety modes and filters are applied
- Role model safe behaviour and privacy awareness. Talk to children about safe use, for example ask permission before taking a child's picture even if parental consent has been given.

• Make use of conversations and meetings with parents to inform your understanding of how technology is used within the home and the context of the child with regards to technology.

Personal mobile phones and other internet-enabled devices – staff and visitors

- Personal mobile phones and internet enabled devices are not used by staff during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe place e.g. staff room.
- Personal mobile phones are stored in staff cupboard
- In an emergency, personal mobile phones may be used in the privacy of the office with permission.
- Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.
- Members of staff do not use personal equipment to take photographs of children.
- Parents/carers and visitors do not use their mobile phones on the premises. There is an exception if a visitor's company/organisation operates a policy that requires contact with their office periodically throughout the day phones still should be stored away from any areas that children access and setting phone number given to visitors so that they are still contactable. Visitors are advised of a private space where they can use their mobile.
- Medical evidence is required for an exemption such as diabetes where the phone is used to alert the staff member of reduction in sugar levels. Any electronic devices which are used to manage medical needs must be agreed with the manager. A risk assessment for the storage and management of devices is completed by the manager

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to the setting. They do not use their own personal phones to take any images or videos.
- Parents complete a photo consent form prior to their child joining the setting
- Photographs/recordings of children are only taken for valid reasons, e.g. to record learning and development, or for displays, and are only taken on equipment belonging to the setting. Children are given the opportunity to consent to their photograph being taken, even if parent/carer permissions are in place.

- Camera and video use is monitored by the setting manager.
- Where parents request permission to photograph or record their own children at special events, parents are told they do not have a right to share or upload photos of anyone else's children.
- Photographs/recordings of children are only made if relevant permissions are in place by parents or guardians.
- Photographs and Image scraping - Little Oaks recognises that although some apps and websites provide the option of covering children's faces with emojis and stickers, with the development of AI tools, these can be reconstructed with highly accurate facial likeness. Any photographs used for publicity, will have parent consent and safeguarding risks minimised by ensuring that children are not able to be identified. Using stickers and emojis, to protect children's privacy, can be removed or bypassed using editing tools and technology such as image scraping. This means a child's face can still be identifiable or recoverable.
- If photographs are used for publicity, parental consent is gained and safeguarding risks minimised, e.g. children may be identified if photographed in a sweatshirt with the name of their setting on it.

Cyber Bullying

If staff become aware that a child is the victim of cyber-bullying at home or elsewhere, they discuss this with the parents and refer them to help, such as: NSPCC Tel: 0808 800 5000 www.nspcc.org.uk or ChildLine Tel: 0800 1111 www.childline.org.uk

Use of social media

See Staff acceptable use policy

Use/distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images and that it is an offence to groom children online. In the event of a concern that a colleague is behaving inappropriately, staff advise the designated person.