

E-safety (including all electronic devices with internet capacity)

An E-safety audit is included in these procedures to assist with compliance to the revised EYFS 2025.

Online Safety

It is important that children and young people attending Little Poppies Preschool receive consistent messages about the safe use of technology and can 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

- The setting manager at Little Poppies Preschool ensures that all computers have up-to-date virus protection installed.
- Tablets remain on the premises and are stored securely at all times when not in use.

Internet access

- Children never have unsupervised access to the internet.
- Only reputable sites with a focus on early learning are used (e.g. CBeebies).
- Video sharing sites such as YouTube are not accessed due to the risk of inappropriate content.
- 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 at Little Poppies Preschool 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 - default settings tend not to ensure a high level of privacy or security. But remember you still need to supervise children closely.
- 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.
- Check privacy settings to make sure personal data is not being shared inadvertently or inappropriately. (source: <https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-guidance-for-practitioners>)

Personal mobile phones – staff and visitors (includes internet enabled devices)

- Personal mobile phones and internet enabled devices are not to be used by staff at Little Poppies Preschool during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe place e.g, the cupboard (with door closed) or kitchen.
- Personal mobile phones are kept in a tin in the kitchen.
- In an emergency, personal mobile phones may be used 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.
- Designated staff (manager, deputy manager, deputy safeguard lead) are allowed to take their mobile phones on outings for emergency use only.
- 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.

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to 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/carers request permission to photograph or record their own children at special events, general permission is first gained from all parents for their children to be included. Parents are told they do not have a right to photograph or upload photos of anyone else's children.
- Photographs/recordings of children are only made if relevant permissions are in place.
- 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

Staff are expected to:

- understand how to manage their security settings to ensure that their information is only available to people they choose to share information with
- ensure that Little Poppies Preschool is not negatively affected by their actions and do not name the setting
- are aware that comments or photographs online may be accessible to anyone and should use their judgement before posting
- are aware that images, such as those on Snapchat may still be accessed by others and a permanent record of them made, for example, by taking a screen shot of the image with a mobile phone
- observe confidentiality and refrain from discussing any issues relating to work
- not share information they would not want children, parents/carers or colleagues to view
- set privacy settings to personal social networking and restrict those who are able to access
- not accept service users/children/parents as friends, as it is a breach of professional conduct

- report any concerns or breaches to the designated safeguarding lead in their setting
- not engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. There may be occasions when the practitioner and family are friendly prior to the child coming to the setting. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed

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 at Little Poppies Preschool is behaving inappropriately, staff advise the designated safeguarding lead who follow the Allegations against staff, volunteers or agency staff procedure.