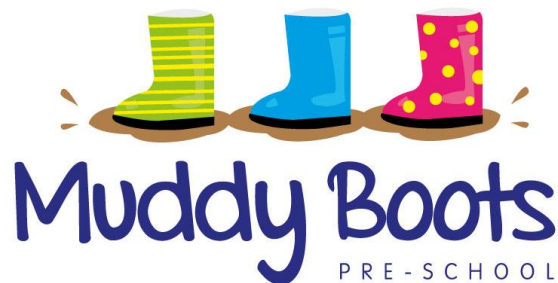# Muddy Boots Pre-School

Child Protection
1.6 E Safety (including all devices with internet capability)

Child Protection

Use of mobile phones and cameras

Policy statement

We take steps to ensure that there are effective procedures in place to protect children, young people, and vulnerable adults from the unacceptable use of internet enabled devices. These include but are not restricted to smart phones, smart watches, recording equipment, cameras and other ICT devices in the setting.

Procedures

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

- The setting manager ensures that 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 are used by staff at home, for the purpose of emailing, Tapestry journal updating, etc.

- Staff follow the additional guidance provided with the system.

Internet access

- Children never have unsupervised access to the internet.

- The setting manager ensures that risk assessments in relation to e-safety are completed.

- 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 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.

Personal Mobile Phones

- 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. The setting manager completes a risk assessment for where they can be used safely.

- Personal mobile phones are stored in an office, which is accessible to adults only.

- In an emergency, personal mobile phones may be used in the privacy of the office with permission from the manager.

- Staff ensure that contact details of the setting (landline telephone number and email address) are known to family and people who may need to contact them in an emergency.

- Staff do take mobile phones on outings. Mobile phones are only switched on and used for the purpose of communication between supervised groups when separated, and in the event of an emergency, and never for personal use.

- Members of staff do not use personal electronic devices for taking photographs of children.

- Parents and visitors are requested not to use their mobile phones whilst on the premises. Signage is displayed requesting this. There is an exception if a visitor's company or organisation operates a lone working policy that requires contact with their office periodically throughout the day.

- Visitors are advised of a private space where they can use their mobile phone.

- Staff have a whistleblowing responsibility to report other staff's misuse of mobile phones during setting opening times.

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to the setting.

- Photographs and recordings of children are only taken for valid reasons, i.e. to record learning and development, or for displays, and are only taken on equipment belonging to the setting.

- Camera and video recording is monitored by the setting manager.

- Where parents request permission to photograph or record their own children at special events, general permission obtained from all parents whose children are to be included. Parents are told they do not have a right to photograph or upload photos of anyone else's children.

- Photographs and recordings of children are only taken if there is parents' written permission to do so (found on the individual child's registration form).

- If a recording device containing photographs and recordings is lost it must be reported to the Designated Safeguarding Lead immediately.