

TURVEY PRE-SCHOOL PLAYGROUP

The Reading Room, High Street, Turvey, Bedfordshire, MK43 8DB

Tel 01234 888970 email: admin@turveypreschool.org www.turveypreschool.org

Registered charity no.295055

Safeguarding children, young people and vulnerable adults procedures

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

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.

Within our Welcome link to Pre-school, all parents will have the Online Safety information pack readily accessible.

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 leader ensures that all computers have up-to-date virus protection installed.
- With the Wifi enabled, the Pre-school Ipad or Preschool laptop are only to be used by a member of staff for demonstration purposes.
- The Ipad can be accessed by children in both the Pre-school and the after school club, with the internet disabled and only downloaded educational games can be accessed, with supervision from staff.
- The Ipad remains on the premises and is stored securely from children.

Internet access

- Children never have unsupervised access to the internet on either the Ipad or Laptop.
- 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 only viewed if they have been assessed prior by a staff member, 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.
- When a child has access to the Ipad, children are sited in an area clearly visible to staff.
- Wifi is to be disabled and checked by an adult before giving to a child.
- 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 – staff and visitors (includes internet enabled devices) – (Please refer to our Smart watch and Mobile phone policy)

- 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 within the office space. Personal devices are not to be in the Pre-school room at any time.
- Personal mobile phones are kept in the upstairs office at all times.
- 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.

- Staff to their mobile phones on outings, for safety reasons but are not to be used for personal reasons or to take any photographs.
- Members of staff do not use personal equipment to take photographs of children. Photos are only to be taken using the Preschool camera or Ipad.
- Parents 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. Visitors are advised of a private space where they can use their mobile. On arrival visitors are asked to place their mobile phone on the shelf in the main room whilst they are on the visit.

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, which include the Pre-school camera and mobile phone.
- Camera and video use is monitored by the setting Leader.
- At special events, if parents would like to photograph or record their child, parents are reminded that their recordings are only for personal use and are not to be displayed on social media.
- Parental consent is gained through our admissions process, if parents approve to photographs/recordings of their children can be used for displays, advertising, social media. The relevant permissions are highlighted within our register so all staff are aware of children with or without 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.
- Photos for scrapbooks are taken using the preschool camera, printed via the Preschool shared laptop and then deleted from both devices once printed.
- Photos used for publicity reasons, are stored on the Finance laptop, which is fully encrypted and password protected. The photos are deleted in a timely manner. (Please refer to the GDPR policy)

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 the organisation 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 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 educator 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 is behaving inappropriately, staff advise the designated safeguarding lead who follows procedure 06.2 Allegations against staff, volunteers or agency staff.