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.

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 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.
- 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
- Video sharing sites such as YouTube are only used to watch videos that compliment the lesson that is being taught or for storytelling videos where we do not have that specific book. Children are supervised while watching these videos at all times.
- 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 – staff and visitors (includes internet enabled devices)

- Personal mobile phones and internet enabled devices are stored in the office during working hours. Staff may use their mobile phones if needed, with permission, in the office, and when it does not impact the safety of the children due to ratios by leaving the classroom. The setting manager completes a risk assessment for where they can be used safely.
- Personal mobile phones are stored in labelled pockets in the office so that it can be seen if a mobile phone has been removed from there.
- Staff are permitted to wear smart watches during working hours **IF** they **DO NOT** have photo taking capabilities. If this is the case, they are to be left at home. If they have been accidently worn to work, they must be handed to the manager and be locked away securely until the end of work.
- Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.
- Staff take one personal mobile phone on outings so that may contact an emergency contact or the emergency services in an emergency. Parent/child emergency contacts are not stored on the mobile phone but are kept in the bag that is taken on outings which includes the first aid kit.
- Members of staff do not use personal equipment to take photographs of children.
- Parents and visitors are asked to not use their mobile phones on the premises unless it is an emergency. If this is the case, they can use the office privately, with permission or take their phone to use off the premisses. 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 in the office where they can use their mobile.

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to the setting however, we use a personal digital camera owned by a member of staff to take photographs for the website and for "profession photos" (eg graduation photos) which we sell to parents. We have our own SD card that is used for this camera so that images of the children are not stored on a personal SD card. This cards stays at the setting when the camera is taken home.

- 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.
- Camera and video use is monitored by the setting manager.
- Where parents 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 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, 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
- be mindful of who they accept as friends eg parents/professionals, as it could be breach of professional conduct. Staff should refer to the "Staff Code of Conduct" document for more information on this.
- report any concerns or breaches to the designated safeguarding lead in their setting

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 the section "Ensuring safe staff – Managing alegations" in the settings Safeguarding and child protection policy.