E-Safety Designated person – Emma Middleton

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 Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting.

Procedures

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used by staff and children.
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- All computers have virus protection installed.
- The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.

Internet access

- Children do not normally have access to the internet and never have unsupervised access.
- The designated person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.
- Children are taught the following stay safe principles in an age appropriate way prior to using the internet;
    - only go online with a grown up
    - be kind online
    - 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
    - Adults will share stories around online safety eg Smartie the penguin.
- Designated persons will also seek to build children's resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age appropriate ways.

E-SAFETY POLICY

- If a second hand computer is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it.
- All computers for use by children are located in an area clearly visible to staff.
- Children are not allowed to access social networking sites.
- 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.
- Suspicions that an adult is attempting to make inappropriate contact with a child online is reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk.
- The designated person ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.
- If staff become aware that a child is the victim of cyber-bullying, they discuss this with their parents and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk.

Email

- Children are not permitted to use email in the setting. Parents and staff are not normally permitted to use setting equipment to access personal emails.
- Staff do not access personal or work email whilst supervising children.

Mobile phones – children

- Children do not bring mobile phones or other ICT devices with them to the setting. If a child is found to have a mobile phone or ICT device with them, this is removed and stored in the office until the parent collects them at the end of the session.

Mobile phones / Digital Watches – staff and visitors

- Personal mobile phones are not used by our staff on the premises during working hours. They will be stored in the locked staff room.
- Technology is getting more and more smarter. We encourage the correct use of technology not only with staff but with children too. They need to see it being used responsibly. Digital watches are permitted, but staff must not become distracted by notifications. If this is misused then the policy will be reviewed and staff will be asked to switch off the Bluetooth.

E-SAFETY POLICY

- Due to the location of the staff room, where staff mobile phones are kept, notifications are NOT received inside the nursery building because Bluetooth cannot connect. Connectivity can only occur in the garden. Management will monitor this situation overall.

- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the manager.

- Our staff and volunteers ensure that the setting telephone number is known to family and other people who may need to contact them in an emergency.

- Parents and visitors are requested not to use their mobile phones / digital watches whilst on the premises. We make 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 will be advised of a quiet space where they can use their mobile phone, where no children are present.

- These rules also apply to the use of work-issued mobiles, and when visiting or supporting staff in other settings.

Camera, videos and Digital Watches

- Our staff and volunteers must not bring their personal cameras or video recording equipment into the setting.

- Photographs and recordings of children are only taken for valid reasons i.e. to record their learning and development, (eyLog) or for displays within the setting, with written permission received by parents (see the Registration form). Such use is monitored by the manager.

- Where parents request permission to photograph or record their own children at special events, general permission is gained from all parents for their children to be included. Parents are advised that they do not have a right to photograph anyone else's child or to upload photos of anyone else's children, especially on any social networking sites.

- If photographs of children are used for publicity purposes, parental consent must be given and safeguarding risks minimised, for example, ensuring children cannot be identified by name.

Electronic learning journals for recording children's progress

- Tablets are used in conjunction with eyLog. An app (SureLock) is used to ensure members of staff cannot access any other settings including the internet from the tablet.

- Staff adhere to the guidance provided with the system at all times.

Use and/or distribution of inappropriate images

E-SAFETY POLICY

- Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately, the Safeguarding Children and Child Protection policy, in relation to allegations against staff and/or responding to suspicions of abuse, is followed

- Staff are aware that grooming children and young people on line is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).

Further guidance

- NSPCC and CEOP *Keeping Children Safe Online* training: www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/

Using Android Tablet's / Smart Board within the setting.

- Children will only have access to the Internet under staff supervision. Under no circumstances will any child be left alone while using the Internet.

- Children and staff are not permitted to access chat rooms or engage in web surfing for personal use.

- The iPads are stored securely in the office at the end of the day. No iPad may be used in toilets or nappy-changing areas or discreet areas of the nursery eg book corner. Nursery Practitioners must behave responsibly with iPads as pieces of delicate electrical equipment, protecting them from damage and ensuring they pose no physical risk to children.

- Time restrictions when using the tablets/smart board will be applied within the setting. 5 minutes for each child. Sand timer will be used.

- Photos stored on the iPad are never uploaded to any part of the Internet.

- All iPads used in the setting have PIN-protected 'Restrictions' on web content and apps. In-App purchases are 'OFF', and Require Password is set to 'Immediately'

- In order to ensure that no photos are being uploaded, e-mail 'sent' lists and web histories on the iPad are never cleared so that they may be checked by the manager.

- The SmartBoard will have internet access, and will only be used to extend interests or children's knowledge. The board is password protected, and has a filtering system blocking any inappropriate materials. Staff will always supervise when in use.

Signed on behalf of the nursery......*Emma Middleton*.......Date:…… August 2021…….