The right start for under 5s

fenniesday nursery & preschool

Online safety (including mobile phones, Smart watches, and cameras)

Safeguarding and welfare requirement 2017: Child protection 3.4.
The safeguarding policy and procedures must include an explanation of the action to be taken when there are safeguarding concerns about a child and in the event of an allegation being made against a member of staff, and cover the use of mobile phones and cameras in the setting.

This procedure also links to:

- Safeguarding children procedure
- Staff usage agreement
- Tapestry policy
- iPad signing in sheet
- Acceptable internet use policy
- Whistleblowing procedure

Procedures

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.

Our designated safeguarding leads responsible for coordinating action taken to protect children are:

Insert name here
Insert name here
Insert name here

Our online safety advocate is: Insert name here

Our Tapestry coordinator is: Insert name here

Information Communication Technology (ICT) equipment

- We aim to completely avoid the use of staff using any personal equipment or devices to take photos or recordings of children, and to always use nursery

provided equipment or communication channels. Use of personal devices can undermine the wider safeguarding culture within our organisation.

- 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 internet is not to be used to watch television programmes, but can be used to view educational clips and play interactive educational games.
- If staff access the internet with children for the purposes of promoting their learning, written permission is gained from parents who are shown this policy.
- 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. A risk assessment template is available here: https://www.safeguardingsheffieldchildren.org.uk/dms/safe/management/corporate-communications/documents/Early-Years-and-Childcare/Early-Years-and-Childcare-Settings-Online-Safety-Self-assessment-Tool/Early%20Years%20and%20Childcare%20Settings%20Online%20Safety%20Self-assessment%20Tool.doc

Children are taught the following stay safe principles in an age appropriate way prior to using the internet:

- only go on line with a grown up
- be kind on line
- 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
- 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.
- 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 on-line 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.
- Staff send personal information by encrypted email and share information securely at all times.

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 a locked drawer until the parent collects them at the end of the session.

Mobile phones – staff and visitors

- Personal mobile phones are not used by our staff on the ground and first floor of the premises during working hours. They are able to use their phones on the second floor of the building where the staff room is located. Phones will be stored in staff lockers in the staff room opposite the nursery office during operational hours.
- 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.
- When going on outings, staff must take the nursery outings phone, which does not have camera or internet access. The nursery office mobile phone must not be taken, nor should staff use their own phones.
- Parents and visitors are requested not to use their mobile phones 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.

Mobile phones – Epsom head office staff

- Mobile phones are not to be used while walking around the nursery and can only be used when in the head office section of the building.

- In an emergency, personal mobile phones may be used in an area where there are no children present.
- Head office staff must ensure that the office or nursery telephone number is known to family and other people who may need to contact them in an emergency.
- Mobile phones must be left inside head office when walking around the nursery and in and out of the nursery rooms.
- These rules also apply to the use of work-issued mobiles, and when visiting or supporting staff on other sites.

Smart watches

We believe our staff should be completely attentive during their hours of working to ensure all children in the nursery receive good quality care and education. To ensure the safety and well-being of children, we do not allow the use of mobile phones and smart watches during working hours. We use mobile phones supplied by the nursery to provide a means of contact in certain circumstances, such as outings.
We require our staff to be responsible and professional in their use of mobile phones and smart watches.
We ask parents and visitors to also respect and adhere to our policy.

Arrangements
Staff must adhere to the following:

- Smart watches can only be used on a designated break and then this must be away from the children, in the staff room or off the premises
- Smart watches should be stored safely in staff lockers or in the mobile phone box at all times during the hours of your working day.
- During outings, staff will use mobile phones belonging to the nursery wherever possible.
- If any of the above points are not followed then the member of staff involved will face disciplinary action, which could result in dismissal.

Cameras and videos

- Our staff and volunteers must not bring their personal cameras or video recording equipment into the setting (this includes cameras and video apps on mobile phones and smart watches).
- Photographs and recordings of children are only taken for valid reasons i.e. to record their learning and development, 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.
- 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 or through being photographed in a sweatshirt with the name of their setting on it.

Social media

- Staff are advised to manage their personal security settings to ensure that their information is only available to people they choose to share information with.
- Staff should not accept service users, children and parents as friends due to it being a breach of expected professional conduct.
- In the event that staff name the organisation or workplace in any social media they do so in a way that is not detrimental to the organisation or its service users.
- Staff observe confidentiality and refrain from discussing any issues relating to work
- Staff should not share information they would not want children, parents or colleagues to view.
- Staff should report any concerns or breaches to the designated person in their setting.
- Staff avoid personal communication, including on social networking sites, with the children and parents with whom they act in a professional capacity. If a practitioner and family are friendly prior to the child coming into the setting, this information is shared with the manager prior to a child attending and a risk assessment and agreement in relation to boundaries is agreed.

Electronic learning journals (Tapestry) for recording children's progress

- Practitioners seek permission from the nursery management team prior to using any online learning journal.
- A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
- Staff adhere to the guidance provided with the system at all times.

Use and/or distribution of inappropriate images

- 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).
- Photos should not be emailed from the nursery tablets / cameras but instead be transferred by cable. Photographs should be deleted from all devices one week after being taken.

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/

This policy was adopted on	Signed on behalf of the nursery	Date disseminated to staff	Date for review
March 2019			*March 2020*