Safeguarding and Welfare Requirement: Child Protection

The safeguarding policy and procedures must include an explanation of the action to be taken 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.

Happy, Confident, Independent.

Children develop a sense of belonging, respect and autonomy of voice through a varied and well-directed early education.

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

Procedures

- Our designated person (manager/deputy) responsible for co-ordinating action taken to protect children is:
  Lucy Hustler

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.
- 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.
- 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 [lockers or 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 premises during working hours. They will be stored in [lockers or a locked drawer].
- 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.
- If our members of staff or volunteers take their mobile phones on outings, for use in case of an emergency, they must not make or receive personal calls, or take photographs of children.

- 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.

Cameras and Videos

- 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, or for displays within the setting, with written permission received by parents (see the Consent 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.
- Managers seek permission from the senior 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.
    - We use the 'LEARNINGBOOK' digital learning journeys. Established in 2012, Learningbook is an Early Years ICT Provider based in Cheshire. The Company was set up by a team of early years

educational professionals and a team of IT experts, headed up by Dr James Huntington, the current Managing Director which is hosted on secure dedicated servers based in the UK.

- Information on learning journals is not stored on the setting computers or tablets.
- Our SmartTablet only runs LearningBook. It's not possible to install any other apps or software onto the device so you can't link to the Internet, e-mail or Facebook to share the information.
- There is no way for data to be sent anywhere outside of LearningBook. Data, including photos and videos, cannot be downloaded, transmitted or transferred anywhere.
- Access to information stored on the Learningbook can only be gained by unique user ID and password.
- Learning journals can be accessed from any computer by using a password protected login.
- Parents can only see their own child's information and are unable to login to view other children's Learning Journeys.
- Staff use tablets to take the photographs for observations but these will not be stored on the device. Photos will be uploaded to the portal once logged onto the Administration portal and then deleted from the device.
- Staff access is secured by a unique user ID and password which they must not share with anyone else.
- Staff access allows input of new observations and photos or amendment of existing observations and photos.
- Parent access allows input of new observations and photos or the addition of comments on existing observations and photos – parent log-ins do not have the necessary permission to edit existing material.
- Observations input into the Learningbook system are moderated by a senior member of staff before being added to the child's Learning Journey.
- Parents are asked to sign a Consent Form giving permission for their child's image to appear in other children's Learning Journeys, and to protect images of other children that may appear in any photos contained in their child's Learning Journey.
- New observational entries to a child's Learning Journey will usually be uploaded within two weeks of the observation being made.
- Observations are written in the present tense.
- In all written observations, other children are referred to by an initial and not by name. An exception to this may be where siblings are present in the same photograph.
- Learningbook is not used as a general communication tool between Nursery and home. A child's learning journey is a document recording their learning and development and parents may add comments on observations or contribute photos, videos or information about activities they have been doing at home.
- Parents may contact us through the usual channels for any other day-to-day matters, e.g. absence, lost property, etc.

- Staff are not permitted to take tablets home and they will remain on the premises at all times. They are to be stored in a locked cupboard at the end of each day and over the holidays as a security measure.
- For parents without access to the internet, we will print all the information from Learningbook and put it into a folder.
- Where a primary school also has Learningbook we will, with parental permission, transfer the child's learning journal to the receiving school's Learningbook database according to the directions given on the Learningbook website.

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).

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 by	Ringrose Kindergarten Chelsea
On	11th June 2020
Date to be reviewed	July 2021
Signed on behalf of the provider	
Name of signatory	Lucy Hustler Parker
Role of signatory (e.g. chair, director or owner)	Principal

Other useful Pre-school Learning Alliance publications

- Safeguarding Children (2013)
- Employee Handbook (2012)