Online safety and Data protection policy

Section 3.4/ 3.5 in Statutory Framework in EYFS

Policy statement

In the Orchard Day Nursery, 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.
To ensure our online safeguarding practice is in line with statutory requirements and best practice we will access the guidance 'Safeguarding children and protecting professionals in early years settings: online safety considerations'. Furthermore, we will share with our staff the 'Online Safety Guidance for Practitioners' guidance (please refer to further guidance section).

Procedures

- Our designated person (manager/deputy) responsible for co-ordinating action taken to protect children is:
- **Alia Smith & Gayathripooja Ramakrishnan**

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting and with all the pat tests are allowed to be used by staff and children.
- The designated person is responsible for ensuring all ICT equipment are 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, such educative videos or digital British book like the Gruffalo, staff must get permission previously by the manager, or DSL in charge.
- The designated person has overall responsibility for ensuring that children and are safeguarded and any 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 all **"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 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 always send personal information by encrypted email and share information securely.
- Information such policies, staff meeting, supervision minutes or any other related to the daily service of the setting will be shared with the member of staff only by the corporative e-mail. Also, who is sending the e-mail who is most of the time is the manager, deputy or third in charge, will check and guarantee the children's name are not written in the document to be send.

- If for any reason a member of staff must to open the personal email, bust to inform and get authorization by the manager.

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 mangers office 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 their locker in the staff room.
- In an emergency, appointment call holding or familiar situation, the personal mobile phones can be used in the office, where children are not 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, same as the setting has a template with all the emergency and next kin person of all members of staff.
- 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, for example the Fire alarm inspector, or safety and infrastructure officer, , however they must to call the manager and take any picture of the devices or electric stuff in presence of the manager.
- We follow a (Mobile-off) police and around the setting are some notices displays regarding to keep informed all parents, and visitor.
- Parents are not allowed to take picture or videos of the children if there is a celebration of the parents visit the nursery to be part of educative activities.
- 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, volunteers, agencies, or parents 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 Registration form). Such use is monitored by the manager.

- The picture for observations or developing tracking will be taken with the iPad for the setting.
- Where there are special events, the picture will be taken by the Ipad and share in Family app if the child is individual, however if there is a group picture, all the parents must be agreeing a 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.
- The Orchard Day Nursery Kew, prevent any kind of incorrect use of photos or digital information of children. However, the nursery will not be able to control the use of the group picture once the parents get those by Family App.

Social media - Staff

- 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.
- If 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 an early year's educator 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.
- The Orchard Day Kew holds two corporative accounts as Facebook and Instagram, and with support of the marketing team will update picture of the setting, however never a child picture will be used in the nursery social media before to gain the written permission by parents.
- Staff will update weekly and termly pictures or videos of the children in individual track as part of the following procedure and monitoring of their process.
- The IPads of the nursery will be cleaned at the end of every term. All pictures will be deleted once a new term start.

- Parents can share with staff picture of the children only with “development tracking process” which will require to do an observation of the activity the child is doing at home with parents. However, the picture cannot involve other children.

Social media parents:

The Orchard Day nursery Kew will promote to the families’ campaigns with sensible information about online data and safety protection online. As we know many of our parents are updating picture of children’s journey in general, and the parents has totally autonomic to decided which data is being sharing in a public way, we consider that parents must be aware of all the steps they must to follow to prevent being victim of a digital abuse.
The nursery will promote to the parents the access to free webinars to keep the informed and updated of the risk of sharing picture and data information of children in social media such Instagram or Facebook.

Electronic learning journals for recording children’s progress

- Managers seek permission from the senior management team prior to using any online learning journal different to Educare Tes NDA or Hight speed online training. A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
- Staff adhere to the guidance always provided with the system.

Use and/or distribution of inappropriate images

- Parents are requested to do not share picture of the children by email or Family App (body part, children with not clothes or in nappies). Whenever there is a complain of a bruise or mark identified for parents at home, which was not informed by staff, parents must write back to manager, with no pictures as evidence.
- 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 online is an offence and concerns about a colleague’s or others’ behaviour are reported (as above).

CCTV cameras in settling.

The setting is cover for a set of 7 camaras working 24/7. To which only the manager has access of the videos. The manager is not allowed to be sharing any recording data with other member of staff or with parents. This video will be

used just in case of an investigation as evidence material. Only the DSL officer are allowed to get into the playback of camaras after gained the authorization by the manager.

ICT corner Preschool room

The preschool room children will have access to the ICT corner, as it is part of the "Understand the world" area, which the purpose will be develop vocabulary with them, introduce them to the awareness of electric devices, however, any laptop, or machine with bottoms they will be playing with, will be off and will not have any access with media or internet.

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/

- Safeguarding Children and Protecting Professionals in Early Years Settings Online Safety Considerations for Managers: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776470/UKCIS_Early_Years_Online_Safety_Considerations_for_Managers.pdf

- Safeguarding Children and Protecting Professionals in Early Years Settings Online Safety Guidance for Practitioners: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776473/UKCIS_Early_Years_Online_Safety_Guidance_for_Practitioners_1_.pdf
- Early Years practitioners: using cyber security to protect your settings: https://www.ncsc.gov.uk/guidance/early-years-practitioners-using-cyber-security-to-protect-your-settings

This policy was Adopted on	*June 2025*
Signed on behalf of the nursery	*Alia Smith*
Date of review	*June 2026*
Date of review	*June 2027*