PEMBURY SCHOOL HOUSE NURSERY

CHILD PROTECTION
Online Safety Policy (including 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.
We take steps to ensure children, parents and staff aware of online safety and to minimise the risks to enable the children to thrive in a healthy and safe environment.

Procedures
Information Communication Technology (ICT) equipment
- Only ICT equipment belonging to the setting is used by staff and children.
- All computers have virus protection installed.
- All tablets from the classrooms are to be stored overnight in the office at the end of the afternoon session.

Internet access
- Children do not normally have access to the internet and never have unsupervised access.
- All ICT equipment for use by children, are located in an area clearly visible to staff.
- All ICT programmes used in the setting are purchased and are free of adverts (this is because adverts could contain content that is not age appropriate).
- All tablets used in the setting have strict parental controls, limiting access to age-inappropriate content, setting time limits, only allowing approved educational apps, all staff are trained on proper supervision and online safety practices when using the device with children.

Online Safety
It is important that children and young people attending Pembury School House Nursery receive consistent messages about the safe use of technology and can 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

Email

- Children do not have access go emails within the setting.
- Parents and staff are not normally permitted to use setting equipment to access personal emails.
- Staff do not access personal or work emails 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 safely until the parent collects them at the end of the session.

Mobile phones – staff and visitors

- Personal mobile phones or cameras are not used by staff on the premises during session time. These are stored in the nursery office during session times.
- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the manager.
- 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 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, and they will be locked away in a secure place for the duration of the visit.

Cameras and videos

- 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 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.
- Children are given the opportunity to consent to their photograph being taken, even if parent/carer permissions are in place.

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 manager 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 an agreement in relation to boundaries is agreed.

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/
- Safeguarding Vulnerable Group At 2006
- Data Protection Act 2018
- Freedom of Information Act 2000
- Keeping Children safe In Education 2025
- https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations
- https://www.ncsc.gov.uk/guidance/early-years-practitioners-using-cyber-security-to-protect-your-settings

This policy was updated and adopted by the Trustees of Pembury School House Nursery.

Date: …… Signed on behalf of the Trustees: ……...

Date: …… Signed on behalf of the Nursery: ….……...