



Barn Close Pre-School

Safeguarding children, young people and vulnerable adults' procedures

06.10 E-safety (including all electronic devices with imaging and sharing capabilities)

Online Safety

It is vital that even young children 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 in an age-appropriate manner.

Terms like 'e-safety', 'online', and 'digital technologies' refer to fixed and mobile technologies that individuals encounter, potentially exposing them to risks such as:

- Content: Exposure to illegal or harmful material.
- Contact: Harmful interactions with other users online.
- Conduct: Personal online behaviour that may lead to harm.

Barn Close Pre-school is registered with the ICO regarding holding sensitive information

I.C.T Equipment

- The setting manager, Amy Gepp, ensures that all computers have up-to-date virus protection installed.
- Tablets are used only by staff for observation, assessment, and planning, and for photographing individual children's learning journeys.
- All photographs will be deleted every 4 weeks.
- Tablets will be taken off the premises only by the Manager and will be stored securely when not in use.
- All devices used are password-protected and use two-factor authentication (2FA) to prevent children/visitors from gaining access.

- Ofsted will be notified should the pre-school tablet be lost or stolen.

Internet access

- Children never have access to the internet in the setting
- Children are taught the following stay safe principles in an age-appropriate way:
 - only go online with a grown-up
 - be kind online **and** keep information about me safe
 - only press buttons on the internet to things I understand
 - tell a grown up if something makes me unhappy on the internet
- Role model safe behaviour and privacy awareness. Talk to children about safe use, for example, ask permission before taking a child's picture, even if parental consent has been given.
- Utilise home visits to enhance your understanding of how technology is used within the home and in the context of the child's relationship with technology.

Personal mobile phones – staff and visitors

- Staff are not permitted to use personal mobile phones or internet-enabled devices during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe place
- Personal mobile phones are stored in a lockbox.
- In an emergency, personal mobile phones may be used in private.
- Staff ensure the setting's contact details are known to the family and to anyone who may need to contact them in an emergency.
- Staff do not take their mobile phones on outings.
- Staff members do not use personal equipment to photograph children.
- Parents and caregivers are not permitted to use their mobile phones on the premises.
- Visitors from outside agencies are advised that a private space is available for them to use their mobile devices if required.

Cameras and videos

- Staff members are not permitted to bring their own cameras or video recorders to the setting.
- Photographs of children are taken only for valid reasons, such as recording learning and development or for displays, and are taken using equipment belonging to the setting. Children should consent to their photographs being taken, even if parental or carer permissions are in place.
- The setting manager monitors camera use.
- Where parents/carers request permission to photograph or record their own children at special events, general permission is first gained from all parents/carers for their children to be included. Parents are told they do not have the right to photograph or upload photos of anyone else's children.

Cyber Bullying

If staff become aware that a child is the victim of cyber-bullying at home or elsewhere, they discuss this with the parents.

Use of social media

Staff are expected to:

- understand how to manage their security settings to ensure that their information is only available to people they choose to share information with
- ensure the organisation is not negatively affected by their actions, and do not name the setting
- are aware that comments or photographs online may be accessible to anyone, and should use their judgment before posting
- observe confidentiality and refrain from discussing any issues relating to work
- not share information they would not want children, parents or colleagues to view
- set privacy settings to personal social networking and restrict those who can access
- not accept service users/children/parents as friends, as it is a breach of professional conduct
- report any concerns or violations to the designated safeguarding lead in their setting

- not engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. There may be occasions when the educator and family are friendly before the child comes to the setting. In this case, information is shared with the manager, and a risk assessment and a boundary agreement are established.

Use/distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images and that it is an offence to groom children online. If a colleague is suspected of misbehaviour, staff should advise the designated safeguarding lead, who will follow the procedure for Allegations against staff or volunteers.