Online safety (inc. mobile phones and cameras)

Policy statement

Home from Home Childcarers 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 responsible for co-ordinating action taken to protect children is:

Zoe Shaw

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used by 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.
- Camera's on laptops are to be covered when it is being used where children are present.

Internet access

- Children do not normally have access to the internet and never have unsupervised access.
- 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 online with a grown up
  - be kind online
  - 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.
- 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 emails 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 in the 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 the office and only accessible when the staff leave the building for lunch or on school runs.
- 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, schools 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 required 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.
    - Potential parents that come for a show round or stay and play session, or a parent that has come in for a meeting are required to leave their mobile phones in the office.

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 photo permission form).
- 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 will inform management if they accept service users, children and parents as social media friends.
- 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, staff all have to read and sign the Social Contact Policy when they join the setting.

Electronic learning journals for recording children's progress

- We use the online system BabysDays to record children's progress, daily activities and photographs. All staff and parents have their own unique log in. Parents are explained how the system works when they join the setting and our Assistant Manager goes through any technology guides (if needed). All staff are trained in BabysDays within the first 3 months of them starting at the setting ensuring they understand how to use the system 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 online 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/

Other useful Pre-school Learning Alliance publications

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

Policy links

Our intention is for this policy to be read in conjunction with the following Home from Home Childcare Policies and Procedures:

- Children's Rights and Entitlements
- Safeguarding Children, Young People and Vulnerable Adults
- Online Safety
- Social Contact Policy

	Date:	**By Whom?**	**Comments**
Created	1st November 2019	Zoe Shaw	
Reviewed	4th February 2020	Chrissie Morley + SMT	
Next Review	February 2021		