



## **Online Safety & Acceptable Use (inc. mobile phones and cameras)**

### **Policy statement**

Home from Home Latton Bush 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 **Chrissie Morley**.

### ***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 with the correct filters on devices.
- 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.
- 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](http://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](http://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.
- All technology devices that are used with the setting are subject to filtering and monitoring. All work devices have age restrictions meaning that apps and websites that are above the restrictions are unable to be accessed and require approval by management to access them. Devices are also checked monthly to ensure no filters have been turned off or nothing has been accessed that shouldn’t have been. If during these checks it is found that a device has been used to access something prohibited, then a full investigation will be conducted.
- 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](http://www.nspcc.org.uk), or Childline on 0800 1111 or [www.childline.org.uk](http://www.childline.org.uk).

### ***Email***

Email will be used in the nursery for the purpose of communicating with parents and staff. Staff should consider the following when using email in the nursery:

- Children are not permitted to use email in the setting. Parents and staff are not 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 always share information securely.
- Staff are strictly prohibited from using email on any iPad/tablet in the nursery
- If using the nursery email account staff must ensure they take appropriate measures to protect personal information of children and their families in line with data protection.
- Staff are strictly prohibited from accessing their personal email accounts on nursery devices in the nursery.

### ***Mobile phones – staff and visitors***

- Personal mobile phones and smart watches (that are connected to phones) are not to be 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.
- External agencies/partners who require internet access must do so in accordance with the terms set out in this policy, they may only access the internet in order to make a referral/document their visit on the child's record using their online system.
- 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/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.

### ***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.

### ***Cameras and videos***

- Our staff and volunteers must not bring personal cameras/video recording equipment into the setting.
- Smart watches that can take photos or are connected to phones cannot be worn
- 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 Business 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.
- Staff are unable to access Baby's Days outside of working hours and have restrictions to what information they can see on Baby's Days (for example they are unable to view any personal information such as address, phone numbers and email addresses).

### ***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).

### **Acceptable Use Of Internet In The Setting**

The Internet is a valuable resource for operational productivity, efficient file sharing, EYFS delivery and educational resources. It is the staff member's responsibility that they understand the safe and acceptable use of the Internet in the nursery setting.

- The use of Internet in the setting is only permitted to support the learning and development of the children, or for approved file sharing between nursery devices
- **Staff members are strictly prohibited from attempting to use the Internet for personal reasons, or to share any personal information, photos or videos of children to any other external sources, either via cloud storage, email or other Internet enabled platforms**
- The Business Manager must approve any use of internet sites for learning resources or content on music streaming sites before being exposed to any children or parents
- The use of any personal social networking sites such as Facebook, is strictly prohibited whilst in the nursery, both on nursery ICT equipment and personal devices
- Staff must not post anything onto social networking sites such as 'Facebook' that could be construed to have any negative impact on the nursery's reputation
- Staff must not post anything onto social networking sites that would offend any other member of staff or parent using the nursery
- If staff choose to allow parents to view their page on social networking sites, then this relationship must remain professional at all times, although this is not recommended. See Social Contact Policy.
- If any of the above points are not followed then the member of staff involved will face disciplinary action, which could result in dismissal

### **Nursery Management Suites**

Personal Data will be stored on a nursery management suite, which uses dedicated secure servers to store information on the database. All the information is encrypted to ensure absolute safety and security of information. None of the information is stored locally on any nursery computers or devices. Staff should consider the following when using their nursery management suite:

- This suite contains confidential information about the children and their families, including names, addresses, medical info and customer accounts
- Data is not to be transferred to any personal external storage device without the consent of the Nursery Manager
- Personal information relating to a child, parent or staff member must never be shared via the Internet
- Only devices approved by the ICT Coordinator can be used to access the nursery management suite server

## **Cloud Storage**

Cloud storage solutions are becoming more commonly used with computing technology. They enable easy sharing of information between devices, which can increase productivity and efficiency in any workplace. Staff should consider the following when using any cloud storage platforms in the nursery:

- iCloud is used to automatically share photos and videos between all nursery devices. This means photos taken on iPads will be available on other iPads or computers
- Staff are strictly prohibited from attempting to use their own cloud storage/sharing accounts on any iPads or other nursery devices
- Staff are strictly prohibited from attempting to link the nursery cloud storage systems to their own personal devices
- Staff are strictly prohibited from attempting to link any nursery devices to their own personal cloud storage accounts.

## **E-Safety Incident Reporting Procedure**

In the event of any breach of this policy, incidents should be reported to the Nursery Manager immediately. The incident should then be reported to both the ICT Coordinator and the Lead Practitioner for Safeguarding to ensure the incident is dealt with in an informed and fair manner. Any breach of the policies and procedures in this document will be logged as allegations against staff members and dealt with accordingly. Should the incident in question be deemed as a safeguarding breach then this will be considered gross misconduct and members of staff may be dismissed

## **Policy links**

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

- Children's Rights and Entitlements
- Safeguarding Children and Child Protection Policy

- Social Contact Policy

	<b><u>Date:</u></b>	<b><u>By Whom?</u></b>	<b><u>Comments</u></b>
<b>Created</b>	22 <sup>nd</sup> January 2025	Rachel Simms	New Setting Policy
<b>Next Review</b>	January 2026		