



High Legh Preschool Nursery - E Safety Policy

Policy Statement

High Legh Preschool Nursery will take steps to ensure that there are effective procedures in place to protect the children in our care from the unacceptable use of Information Communication Technology (ICT) or exposure to inappropriate materials in the setting.

Aims

- To offer guidance to the staff at High Legh Preschool Nursery to ensure that they can provide a safe and secure online environment for all children in their care.
- To raise awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many educational and social benefits.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the nursery.

Internet access

Internet provision is essential to the running of the setting, it not only allows for communication with parents and carers but also provides access to a wealth of resources, support and potentially the use of online tools for staff to track and share children's achievement. Care is taken to ensure that safe and secure internet access, appropriate for both adults and children, is made available to the setting.

- Only ICT equipment belonging to the setting is used by staff and children.
- All computers have virus protection installed. • Children do not normally have access to the internet and never have unsupervised access.
- Safety settings are set to ensure that inappropriate material cannot be accessed
- All staff have a shared responsibility to ensure that children can use the internet and related technologies appropriately and safely as part of the wider duty of care to which all adults working with children are bound.
- The Designated Safeguarding Lead has overall responsibility for ensuring that children are safeguarded and risk assessments to online safety are completed.

Email use

- Children are not permitted to use email in the setting
- Staff are not permitted to access personal emails on the setting's devices.

- If staff are required to send an email regarding any issue at Preschool, the settings email address will be used. All emails should be professional in tone and checked carefully before sending, just as an official letter would be.
- Staff always send personal information by encrypted mail and share information securely.

Use of Social Networking Sites (advertising or parental contact)

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. It is recommended that staff members of High Legh Preschool Nursery maintain a professional distance with parents and former parents and pupils of the nursery and do not link their personal social networking account with those of parents and former parents and pupils. Due to High Legh being a small rural area staff members may have friends who become connected with the nursery. Staff must be aware that their personal posts may influence the reputation of the setting. Staff will observe confidentiality and not discuss any issues relating to work. If staff name High Legh Preschool Nursery in any social media, they do so in a way that is not detrimental to the setting or its users. Staff should report any concerns or breaches to the designated person. Staff are aware that grooming children and young people on-line is an offence and concerns about a colleague's behaviour should be reported to the designated person. Disciplinary proceedings will be followed in the event of an inappropriate opinion, message, photo etc. being displayed on social networking accounts. Under no circumstances must an identifiable photograph of a child in our care be used on a staff members social media site. Parents' permission will be sought to allow images of their child to be displayed on our own Nursery Facebook page or images used to promote the Nursery to the public.

Mobile/Smart Phones

- Staff personal mobile phones are permitted on setting grounds, but are to be used during break times only, within designated areas away from children.
- Personal mobile phones must never be used to contact children or their families, nor should they be used to take videos or photographs of children. Setting issued devices only should be used for this purpose and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted.
- Parents/Visitors are requested not to use their mobile phones whilst on the premises.

Photographs and Video Digital photographs and videos are an important part of the learning experience in early years settings and, as such, staff have a responsibility to ensure that they not only educate children about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and children about the use of digital imagery and videos.

- Written consent must be obtained from parents or carers before photographs or videos of young people will be taken or used within the setting, including displays, learning journeys, setting website and other marketing materials.
- Staff will ensure that children are at ease and comfortable with images and videos being taken.
- Staff must not use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of children.

- Setting cameras, devices and video cameras should not leave the premises unless all data has previously been deleted.
- Where parents request permission to photograph or video their own child at special events, general permission is gained from all parents for their child 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 child.
- 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 policy in relation to allegations against staff is followed.

Laptops/iPads/Tablets

The Manager will ensure that any devices that are purchased second hand or donated to the setting has no inappropriate material stored on it before the children use it. Staff Use:

- Where staff have been issued with a device (e.g. setting laptop) for work purposes, personal use whilst off-site is not permitted unless authorised by the Nursery Manager. The settings laptop/devices should be used by the authorised person only.
- Staff are aware that all activities carried out on setting devices and systems, both within and outside of the work environment, will be monitored in accordance with this policy.
- Staff will report any concerns they have about a colleague's or other's behaviour regarding the content or inappropriate use of the setting's devices.

Children's Use:

- All computers for use by the children are in an area clearly visible to staff.
 - Laptop, iPad or tablet use must always be supervised by an adult and any games or apps used must be from a pre-approved selection checked and agreed by the Manager
 - Online searching and installing/downloading of new programmes and applications is restricted to authorised staff members only. Children should not be able to search or install anything on a setting's device.
 - 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 online.
- Applications (Apps) for recording pupil progress in recent years, a few applications (apps) for mobile devices have been launched which are targeted specifically at Early Years Practitioners and settings. Many of these apps allow staff to track and share a child's learning journey online with parents and carers, usually in the form of photographs and text. Such tools have considerable benefits, including improved levels of

engagement with parents and a reduction in paperwork, but careful consideration must be given to safeguarding and data security principles before using such tools.

- Personal staff mobile phones or devices (e.g. iPad or iPhone) should not be used for any apps which record and store children's personal details, attainment or photographs. Only setting issued devices may be used for such activities, ensuring that any devices used are appropriately encrypted if taken off site. This is to prevent a data security breach in the event of loss or theft.
- Assessments of children's learning will not be stored on personal devices belonging to staff. These must be completed on the setting's devices; permission will be sought from the Nursery Manager before using the setting's devices.
- Before purchasing or accessing any apps for staff or children's use, the Nursery Manager must have a clear understanding of where and how children's data will be stored, including who has access to it and any safeguarding implications.
- Please note: The Nursery Manager is ultimately responsible for the security of any data or images held of children within the setting.
- Sensitive data, photographs and videos of children are not stored on setting devices which leave the premises (e.g. laptops, mobile phones, iPads, USB Memory Sticks etc.) unless encryption software is in place.

*Incident Reporting E Safety Incident Log Details of all E Safety incidents to be recorded by staff and monitored monthly by the Nursery Manager in the following format;

Date of Incident Name of individual(s) involved

Device number/location

Date of Incident Actions and reasons

Confirmed by