e-Safety

The Little Learners e-Safety policy covers the safe use of the internet and electronic devices such mobile phones, tablets, smart watches, e-readers, electronic dictionaries, digital cameras and laptops. These technologies are considered to be an everyday item in today's society and even children in early year's settings may own and use online personal devices regularly.

We recognise that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions, as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in our nurseries in order to educate and protect children in their care. Staff also need to be aware of how their online behaviour can impact their professional role.

Images and data stored on these devices is treated as personal data under the General Data Protection Act (GDPR) and the Data Protection Act 2018 (DPA). This policy also links with our Safeguarding and Child Protection policy. This policy sets out Little Learners approach to e-Safety.

1. Why the internet and digital communications are important

The internet is now regarded as an essential resource to support teaching and learning and computer skills are vital for accessing life-long learning and employment. It is important for children to learn to stay safe from an early age. Little Learners can play a vital part in starting this process.

In line with other policies that protect children from other dangers, there is a requirement to provide children with a safe internet environment and a need to begin to teach them to be aware of and respond responsibly to possible risks.

We have a duty of care to ensure children in our nurseries are not exposed to inappropriate information or materials.

2. How We Make Sure Our ICT Systems Are Safe to Use

ICT systems are owned by Little Learners and appropriate software has been installed to ensure safe internet use.

Anti-virus protection and malware protection is installed on computers and devices. Virus protection is updated regularly.

Where it is planned to use online learning as part of the curriculum, internet access will be tailored expressly for educational use and include appropriate filtering. Further details about the security of ICT systems can be found in LifeLine Projects General Data Protection Regulation policy.

The Nursery Manager and Deputy have access to Little Learners devices that include laptops and mobile phones. These staff also have access to the internet and email accounts and use these devices to manage the day to day running of the nursery.

Practitioners use iPads to record and upload children's observations onto iConnect (an online learning journal). Information recorded on iPads is deleted daily.

Where staff discover unsuitable sites have been accessed, they must report the incident to:

- the Designated Safeguarding Lead.
- Integrity (IT security and maintenance providers) on 08000 80 30 30 so that filters can be reviewed
- On SharePoint

Once an incident has been reported on SharePoint, an investigation will take place to determine how the breach will be managed, and whether it is reportable to the Information Commissioner's Office.

3. How We Manage Children's Access to the internet

a) Internet access is designed to enhance and extend education.

b) We ensure that children know how to ask for help if they come across material that makes them feel uncomfortable.

c) We ensure that the copying and subsequent use of internet-derived materials by staff complies with copyright law.

d) Staff only use age-appropriate, authorised sites to access teaching and learning materials for children.

4. Information Security – Email

Sending personal, sensitive, confidential information by email must be avoided wherever possible as its security cannot be guaranteed.

If it is necessary to send information in this way, and secure email cannot be used, we will make sure the personal information has been either password protected or de-personalised.

4.1   Procedures for Staff When Sending Information by Email

a) Staff must not use their personal email addresses to communicate with parents.
b) Wherever possible, use secure email such as Egress, for sending confidential information.
c) Where secure email is not used, ensure all recipients need to receive the information - think twice before responding to a group email or copying others in.
d) Confirm the name, department and email address of the recipient (to ensure the information is emailed to the correct recipients).
e) Use a flag to mark the message 'confidential'.
f) Do not include personal or confidential information in the subject field.
g) Ask the recipient to confirm receipt of the email.

h) If sending any email to multiple recipients outside of the nursery, use the blind copy (BCC) facility so recipients can't view other recipients' email addresses (which, depending on the subject of the email, could constitute personal information).

i) The forwarding of chain letters is not permitted.

5. Published content (network or online)

a) LifeLine Projects will not publish staff or children's personal contact information online.

b) Written permission from parents/carers will be obtained before images/videos of children are published online.

c) Images or videos that include children will be selected carefully.

d) Children's full names will not be used anywhere online, particularly in association with photographs.

In liaison with the Communications Manager, Nursery Managers will ensure that published content is accurate and appropriate.

6. Staff use of social media

Social media refers to a variety of online internet applications that enable users to create their own content and interact with other users. Examples of social media providers are Facebook, Google, Instagram, LinkedIn and Twitter.

a) Staff must not post anything on social media that is likely to have an impact on Little Learner's reputation, or relate to our nurseries or any children attending the nursery in any way.

b) Staff must not post anything on to social media sites that could offend any other member of staff or parent using the nursery.

c) If staff choose to allow parents to view their page on social media this relationship must remain professional at all times.

d) No member of staff is permitted to discuss or post on social media any information relating to any part of their work at Little Learners, including but not exclusive to, comments about other staff, children, the working day and practices. This includes but is not exclusive to Facebook and Twitter and is in line with our Safeguarding and Children Protection and Data Protection policies.

e) Staff can only access social media during breaks, either in the designated area, or off the premises.

f) In order to maintain professional boundaries, staff should not accept personal friend invitations from parents of the nursery, unless they know them in a personal capacity prior to starting work at

g) the nursery, for example a relative or close friend. Existing online friendships are required to be signed off by the Nursery Manager.

h) Staff are advised to be cautious and mindful when accepting friend requests from colleagues.

i) Staff members are advised to review their social media privacy settings and be aware of what information can be viewed on their profile. The following contains useful factsheets about privacy settings - https://ico.org.uk/your-data-matters/online/social-media-privacy-settings/

j) Staff at Little Learners must not display the nursery name anywhere on their social media profiles. This is for safeguarding purposes. However, staff are encouraged to 'like' the Little Learners Facebook page.

k) Staff must be mindful that everything shared online can be 'public', even with the strictest privacy settings.

l) Staff may be required to remove internet postings which are deemed to constitute a breach of this policy.

m) Staff should notify the Nursery Manager immediately if they become aware of any social networking activity that identifies Little Learners nurseries, staff, children or families in a detrimental way.

n) Personal use of social media is not permitted using Little Learners computers, networks and other IT resources and communications systems.

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

7. Little Learners Facebook page

a) Each nursery has a public Little Learners Facebook page that is used for extending parent partnership through:

- Promoting certain events at the nursery, or giving news updates.
- Giving hints and tips on activities to extend children's learning at home.
- To show photos of activities, trips or special events.

b) During the Registration Process parents are asked to give permission for their child to appear on social media. There is absolutely no obligation for parents/carers to give permission. Children's pictures will only appear on the page if prior permission has been given by parents/carers.

c) The Nursery Managers and the Communications team are the page administrators for Facebook.

d) We welcome appropriate parents and staff comments on the Facebook page. However, the administrators reserve the right to remove any comments at any time.

8. Parents Use of Social Media

a) We ask parents to respect our Staff Social Media policy and professional boundaries and not send personal friend invitations to staff members unless they know them in a personal capacity prior to joining the nursery, for example as a relative or close friend.

b) When photographs are taken by parents at Little Learners events, we request, at the beginning of the event, that parents keep them for personal use only and do not post them on social media as they may contain a child or children whose parents do not wish them to appear online.

c) If parents see something online that is linked to Little Learners that they don't feel comfortable with, we request that they notify the Nursery Manager immediately so the appropriate action can be taken.

9. Managing emerging technologies

Emerging technologies will be risk assessed before use is allowed.

10. Use of mobile phones and other electronic devices with imaging or sharing capabilities

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 camera's, mobile phones and other electronic devices with sharing capabilities in the setting. Our procedures are detailed in our Mobile Phone and Electronic Device Use policy.

11. e-Safety Complaints

a) We will follow our complaints policy when dealing with e-safety complaints.

b) The Nursery Manager is responsible for dealing with complaints.

c) Any complaint about staff misuse must be referred to the Nursery Manager.

d) Complaints of a child protection nature will be dealt with in accordance with our child protection procedures – see Safeguarding and Child Protection policy.

This policy meets the requirements of the Statutory Framework for the EYFS 4TH January 2024

Date policy last reviewed/updated	June 2024	Reviewed by	Julia Ward, Head of Support Services
Date of next review/update	June 2025		