

e-Safety

The Little Learners e-Safety Policy covers the safe use of the internet and electronic devices such as mobile phones, tablets, smart watches, e-readers, electronic dictionaries, digital cameras and laptops. These technologies are an everyday part of modern society, and even children in early years settings may own and use personal online devices regularly.

We recognise that children and staff cannot be completely protected from all online and offline risks. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions, recognise potential risks and feel confident in reporting 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 and responsibilities.

Online safety is recognised as a safeguarding issue. Little Learners is committed to protecting children and staff from risks associated with the use of digital technology, including inappropriate content, cyberbullying, online grooming, misuse of images, data breaches and unauthorised sharing of information.

Images and data stored on these devices are treated as personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy should be read alongside the Safeguarding and Child Protection Policy, General Data Protection Regulation Policy and Use of Mobile Phones and Cameras Policy. Social media expectations for staff, parents/carers and authorised nursery social media accounts are contained within this e-Safety Policy. This policy sets out Little Learners' approach to e-Safety and the safe use of online platforms and digital technology.

This policy incorporates Little Learners' requirements relating to the professional use of social media, the management of nursery social media accounts, and expectations for parents/carers when engaging with social media platforms.

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

Little Learners will follow National Cyber Security Centre (NCSC) guidance for early years providers. This includes:

- Strong passwords and multi-factor authentication where available.



- Restricted access to children's records.
- Regular software updates.
- Secure storage of electronic records.
- Reporting suspected cyber incidents immediately to management.

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

Anti-virus protection and malware protection are 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, including 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/tablets to record and upload children's observations onto Tapestry (an online learning journal). Information recorded on iPads/tablets is deleted weekly.

Staff receive regular online safety and cyber security awareness training to support the safe use of nursery ICT systems.

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

- The Designated Safeguarding Lead (DSL).
- Integrity (IT security and maintenance providers) on 08000 80 30 30 so that filters can be reviewed.
- 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 (ICO).

Suspected cyber security incidents, inappropriate online content, unauthorised access to nursery systems, data breaches or online safeguarding concerns must be reported immediately to the DSL and recorded in accordance with safeguarding and data protection procedures.

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

- a) Internet access is designed to enhance and extend children's learning and development.
- b) Children are supported to understand how to ask for help if they encounter content, images or information that makes them feel uncomfortable, worried or upset.
- c) We ensure that the copying and subsequent use of internet-derived materials by staff complies with copyright and intellectual property laws.



- d) Staff only use age-appropriate, authorised and suitably risk-assessed websites, applications and online resources to support children's learning and development.
- e) Children's use of digital technology is always supervised by staff and forms part of a balanced learning experience alongside physical play, social interaction and outdoor activities.
- f) Any concerns regarding a child's online safety or exposure to inappropriate content will be reported to the Designated Safeguarding Lead (DSL) and managed in accordance with the Safeguarding and Child Protection Policy.

4. Online Safety Safeguarding

Online safety is recognised as a safeguarding issue. Staff must remain vigilant to risks associated with:

- Inappropriate online content.
- Online grooming.
- Cyberbullying.
- Exposure to extremist content.
- Harmful online challenges.
- Misuse of images.
- Data breaches.
- Unauthorised sharing of children's information.

Concerns regarding a child's online experiences, online behaviour or exposure to inappropriate content will be addressed in accordance with the Safeguarding and Child Protection Policy and reported to the Designated Safeguarding Lead (DSL) where appropriate.

Little Learners is committed to promoting the safe and responsible use of digital technology and ensuring that online safety forms an integral part of safeguarding practice throughout the nursery.

5. Information Security – Email

Sending personal, sensitive or confidential information by email should be avoided wherever possible, as the security of email communications cannot be guaranteed.

If it is necessary to send information by email and a secure email system cannot be used, appropriate measures must be taken to protect the information. This includes ensuring that personal information is password protected, encrypted where possible, or de-personalised before being sent.

5.1 Procedures for Staff When Sending Information by Email

- a) Staff must not use their personal email addresses to communicate with parents.
- b) Wherever possible, approved secure email systems or secure file-sharing solutions must be used when sending confidential or sensitive information.



- c) Where secure email is not used, ensure that all recipients need to receive the information. Think carefully before responding to group emails or copying others into correspondence.
- d) Confirm the name, department and email address of the recipient to ensure the information is sent to the correct person(s).
- e) Mark emails containing sensitive or confidential information as '**Confidential**'.
- f) Do not include personal, sensitive or confidential information in the subject line.
- g) Request confirmation of receipt from the recipient where appropriate.
- h) If sending an email to multiple recipients outside the nursery, use the blind carbon copy (BCC) facility so that recipients cannot view other recipients' email addresses. Depending on the subject matter, the disclosure of email addresses may constitute a data protection breach.
- i) The forwarding of chain letters, spam emails or unauthorised mass communications is not permitted.
- j) Staff must immediately report any email sent to an incorrect recipient, suspected phishing email, or potential data breach to the Designated Safeguarding Lead and/or Data Protection Lead in accordance with data protection procedures.

6. Published content (network or online)

- a) LifeLine Projects will not publish staff or children's personal contact information online.
- b) Written consent will be obtained from parents/carers before images or videos of children are published online.
- c) Images or videos that include children will be selected carefully to ensure they are appropriate and do not place children at risk.
- d) Children's full names will not be used online, particularly in association with photographs, videos or other identifying information.
- e) Published images and content will be reviewed to ensure they do not disclose personal information, locations or details that may compromise the safety or privacy of children, families or staff.

In liaison with the Communications Manager, Nursery Managers will ensure that all published content is accurate, appropriate and compliant with safeguarding, data protection and privacy requirements.



7. 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 platforms include Facebook, Instagram, LinkedIn, TikTok, and other messaging or networking applications.

- a) Staff must not post anything on social media that could adversely affect Little Learners' reputation or that relates to the nursery, its children, families, staff or operations.
- 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 limited 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 Child Protection and Data Protection policies.
- e) Staff may only access personal social media during authorised breaks and in designated staff areas or away from the nursery premises.

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

- f) Staff are advised to be cautious and mindful when accepting friend requests from colleagues.
- g) 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/>
- h) 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.
- i) Staff must be mindful that everything shared online can be 'public', even with the strictest privacy settings.
- j) Staff may be required to remove internet postings which are deemed to constitute a breach of this policy.
- k) 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.



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

m) Staff must not:

- Create, share or store images of children on personal devices.
- Communicate with children via social networking sites or personal messaging applications.
- Use disappearing-message applications or functions for work-related communication.
- Share nursery information through private social media groups or messaging platforms unless authorised by Little Learners.
- Use personal devices to take photographs, videos or audio recordings of children.
- Share confidential nursery information, records, observations or safeguarding information through social media or messaging applications.

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.

7.1 Staff Training and Awareness

- All staff will receive regular safeguarding and online safety training as part of their induction and ongoing professional development.
- Training will include online safety, professional conduct online, cyber security awareness, data protection and reporting concerns.
- Designated Safeguarding Leads (DSLs) will maintain up-to-date knowledge of online safeguarding, cyber security risks and emerging technologies.
- Staff must report any online safety concerns in line with the Safeguarding and Child Protection Policy.

Any member of staff suspected of committing a breach of this policy will be required to cooperate fully with any investigation. This may involve providing relevant information, records or access to work-related accounts where appropriate and lawful.

8. Little Learners Social Media Accounts

a) Little Learners maintains official social media accounts and online platforms to support parent partnerships by:

- Promoting events and activities at the nursery and sharing news updates.
- Providing hints, tips and ideas to extend children's learning at home.
- Sharing photographs of activities, trips and special events, where appropriate consent has been obtained.



b) During the registration process, parents/carers are asked to provide consent for their child to appear on social media. There is no obligation for parents/carers to give consent. Photographs or videos of children will only be shared on official Little Learners social media accounts where prior consent has been obtained.

c) The Nursery Managers and Communications Team are the authorised administrators of Little Learners' official social media accounts and are responsible for ensuring content is appropriate, accurate and compliant with safeguarding, data protection and privacy requirements.

d) We welcome appropriate comments from parents/carers and staff on Little Learners' social media accounts. However, administrators reserve the right to remove comments that are considered inappropriate, offensive, defamatory, breach confidentiality, or are otherwise inconsistent with the values and policies of Little Learners.

9. Parents Use of Social Media

- a) We ask parents/carers to respect professional boundaries and refrain from sending personal friend requests to staff members on social media unless they have an existing personal relationship with the staff member, such as a relative or close friend.
- b) When photographs are taken by parents/carers at Little Learners events, we request that they are kept for personal use only and are not shared on social media or other online platforms, as they may include children whose parents/carers have not given permission for their child to appear online.
- c) If parents/carers see anything online that is linked to Little Learners and causes concern, they should notify the Nursery Manager as soon as possible so that appropriate action can be taken.

10. Children's Screen Use

Digital technology may be used to support learning and development where it adds educational value and supports the delivery of the EYFS. Screen use will:

- Be age appropriate.
- Be supervised by staff at all times.
- Complement, rather than replace, active play, outdoor experiences and social interaction.
- Support identified learning outcomes.
- Be used safely, responsibly and with a clear educational purpose.

Little Learners follows current government guidance on screen use in the early years. As a precautionary approach:

- Screen time will be avoided for children under 2 years of age except in exceptional circumstances.
- For children aged 2 to 5 years, screen use within the nursery will be kept to a minimum and used only where it enhances learning and development.



- Screens will never replace high-quality interactions with adults, physical activity, play, exploration and hands-on learning experiences.
- Screens will not be left on in the background and children will not access digital content without appropriate supervision and adult engagement.
- Any digital content used with children must be safe, age-appropriate and suitable for their stage of development.

Staff will monitor and review screen use to ensure children experience a balanced curriculum that promotes their learning, development, wellbeing and physical activity. Children will be supported to develop an awareness of online safety through age-appropriate discussions, activities and guidance from staff.

11. Managing emerging technologies

Emerging technologies, including artificial intelligence (AI) applications, new communication platforms and digital learning tools, will undergo a risk assessment before use within the nursery.

Consideration will be given to:

- Safeguarding implications.
- Privacy and data protection.
- Age appropriateness.
- Content filtering and access controls.
- Supervision requirements.
- Compliance with UK GDPR, the Data Protection Act 2018 and EYFS requirements.

Where appropriate, staff will receive guidance and training on the safe and appropriate use of emerging technologies. Any concerns relating to the use of emerging technologies will be reported to the Designated Safeguarding Lead (DSL) and managed in accordance with safeguarding and data protection procedures.

12. Use of mobile phones, other personal devices and cameras

We take steps to ensure that effective procedures are in place to protect children, young people and vulnerable adults from the inappropriate or unacceptable use of mobile phones, cameras and other personal electronic devices within the setting.

This includes devices capable of capturing, storing, accessing or sharing images, video, audio or online content, such as mobile phones, tablets, smart watches and wearable technology.

Our procedures are detailed in the **Use of Mobile Phones and Cameras Policy**, which should be read alongside this e-Safety Policy, the Safeguarding and Child Protection Policy, and the Data Protection Policy.



13. e-Safety Complaints

- a) We will follow the Complaints Policy when dealing with e-Safety complaints.
- b) The Nursery Manager is responsible for receiving, managing and responding to e-Safety complaints.
- c) Any complaint relating to the misuse of technology, social media, electronic devices or online systems by a member of staff must be reported to the Nursery Manager without delay.
- d) Complaints of a safeguarding or child protection nature will be dealt with in accordance with the Safeguarding and Child Protection Policy and relevant safeguarding procedures.
- e) Concerns relating to online safety, cyber security incidents, data breaches or inappropriate online content will be investigated promptly and managed in accordance with safeguarding, information security and data protection procedures.

This policy meets the requirements of the Early Years Foundation Stage Statutory Framework effective from 1 September 2026.

Date policy last reviewed/updated	17 th August 2026	Reviewed by	Terri Noone - Interim Regional Nursery Manager Jodie Richards – Nursery Manager Charlie Walton – Nursery Manager
Date of next review/update	August 2027		