E-safety Policy and Procedures

Policy statement

At Little Fishes Pre-School we recognise the value information and communication technology (ICT) plays in the learning and development of children. There are, however, potential risks associated with it which must be addressed in order to ensure it is used safely.

This policy aims to ensure the e-safety of all users of the setting whether they be child, parent, staff member or visitor. All adults are entrusted to respect and uphold it in order to prevent any potential risk occurring.

The Designated Safeguarding Lead (DSL) is the e-safety lead at Little Fishes. Any e-safety concerns should be reported to the DSL or their deputy, in line with the Setting's Safeguarding Policy.

Key regulatory requirements

EYFS 3.6: *Safeguarding policies must include … how mobile phones, cameras and other electronic devices with imaging and sharing capabilities are used in the setting.*

Prevent Duty 2023: registered early years childcare settings in England and Wales are required to *have due regard to the need to prevent people from being drawn into terrorism*, including *limiting the use of permissive online environments or other platforms, which can contribute to radicalisation by facilitating exposure to terrorist and extremist content, and enabling networking with likeminded people.*

Procedures

Confidentiality

- Any breaches of confidentiality by an adult/student associated with Little Fishes are strictly forbidden and will not be tolerated.
- All suspected breaches of confidentiality must be reported to the Operations Manager, recorded and acted upon immediately.
- Confidentiality by staff is ensured within their terms and conditions of employment. Thus any breach of confidentiality is considered to be gross misconduct and will result in instant dismissal.

- Students must abide by our Data Protection Procedures. Termination of the placement will result if there is any breach of the agreement along with a notification to their educational establishment.

Use of technology in the setting

- Little Fishes has the use of a PC and one or more tablets within the setting, all of which allow access to the internet via the church WiFi. These are all stored securely, have appropriate security, anti-malware software, filtering and monitoring and are only accessible by adults and used under adult supervision.
- Only age appropriate apps, websites and online tools are used with the children. All are checked prior to use with children including, where relevant, the results of searches.
- Members of staff must not bring their own cameras, video recorders, tablets, laptops or other electronic devices with imaging or sharing capabilities, other than personal mobile phones or smartwatches, into the setting.

Personal mobile phones and smartwatches

- Personal mobile phones that contain inappropriate material must not be brought into the setting.
- Smartwatches must not have image or sharing capabilities enabled if worn in the setting.
- Personal mobile phones belonging to staff are not used on the premises during working hours.
- At the beginning of each session, personal mobile phones are stored in a locked cupboard or on the Manager's desk.
- In the event of an emergency, personal mobile phones may be used with permission from the setting manager.
- If a staff member needs to make or receive a call then permission is sought from the setting manager and the call is made/taken in the lobby.
- Members of staff must ensure that the telephone number of the setting is known to anyone who would be expected to need to contact them in an emergency.
- Members of staff may be asked to take their own mobile phones on outings, for use in the case of an emergency, but they must not make or receive personal calls as this will distract them.
- Members of staff must not use their personal mobile phones for taking photographs of children in the setting, including on outings.

- Parents and visitors are requested not to use their mobile phones or smartwatches (other than to check the time) whilst on the premises except in emergency. There is 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 there are no children present.
- Parents and visitors are required to keep their phones in bags (the bags are locked in cupboard) or in the box on the desk and will be reminded of this requirement when entering the setting.

Communication with parents and carers

- Communication with parents and carers should be professional and take place via official setting communication channels, ie Little Fishes phones or email address.
- Little Fishes email address is password protected. Only the Operations Manager and the Pre-School Administrator know the password and they must not divulge it to any other party, as this would be a breach of confidentiality and treated as such. The email address is available on the Little Fishes website, and parents are also made aware of it via the information sent out on registration.

Use of personal devices for Little Fishes outside the setting

- Little Fishes recognises that personal computers or other devices are used to create working documents for the pre-school in terms of planning, registers and reports for example. Staff may also need to communicate via personal email, text or other message outside of work hours, eg to report absence or arrange sickness cover.
- When using personal devices, the following apply:
  - Staff members who use personal devices for work purposes are required to protect them by secure passwords and to install anti-malware software where available.
  - Correspondence will be written in a polite, respectful and non-abusive manner, with an appropriate use of emotions.
  - Work documents must be placed in locked folders
  - Only acceptable use is permitted
  - Personal details of children, parents or carers are kept to a minimum.
  - Information is not stored on personal devices unless necessary and should be deleted when no longer being used (if necessary, first ensuring it is held securely on Little Fishes devices, church records or on paper).
- The setting has registered with the Information Commissioner's Office as a 'data controller' and meets the Data Protection Act legal requirements.

Social networks

- Little Fishes is a member of Facebook and other social media networks and realises that staff, students and parents may have accounts and that situations may arise when staff/students may be discussed. Staff should not foster online relationships with past or present parents or carers from the setting, including acceptance of "friend requests". If there is a pre-existing relationship, this should be discussed with the DSL and/or the manager, who will consider how this is managed, provide staff with clear guidance and boundaries and record action taken.
- Staff should not compromise professional integrity or bring Little Fishes into disrepute by uploading inappropriate comments or photographs of themselves or others that could be viewed by parents.
- Staff members should ensure the security of their profile has been set correctly and a strong password used so that information remains private.
- We have a Parents WhatsApp group for each academic year, managed by the church's Families Outreach Worker. This is used for sharing information about the setting, such as that a child (not named) who has been in the setting has an infectious illness, and informing parents of church events, as well as for parents to ask questions or discuss issues. Parents are not obliged to join but can opt to join or leave this at any time. At the end of each academic year, it is deleted and a new one started for the next year.

Photographs or video or other recordings

- Photographs or recordings of children are only taken on equipment belonging to the setting or the church, unless written permission has been given, for example for professional photographs.
- Photographs and recordings of children are only taken for valid reasons, eg to record their learning and development, or for displays within the setting or presentations to parents and carers.
- Camera and video use is monitored by the setting manager.
- Parents are given permission to photograph or record their own children at special events. In no event should these be uploaded onto the web.
- Photographs and recordings of children are only taken of children if there is written permission to do so for the purpose required (found on the individual child's Photograph Permission Form).
- Professional photographers are sometimes used in the setting, by agreement of the Operations Manager. Only photographers with DBS clearance will be used and they are not

left alone with any of the children at any time. No photographs of children will be taken without parent or carer permission.

Training

- Staff are provided with appropriate online safety training on induction and at least annually.
- As part of the induction process all staff members are required to sign an Acceptable Use Policy, as shown in the Appendix.
- Children receive age appropriate online safety education throughout the curriculum. This includes staff modelling safe practice when using technology with the children.
- Parents and carers are given support in developing their knowledge of online safety issues for early years children and talking to their children about online safety in an age appropriate way.

Legal framework

- Data Protection Act 2018
- The Computer Misuse Act 1990 (sections 1-3)
- Copyright Design and Patents Act 1998
- Malicious Communication Act 1998 (section 1)
- Obscene Publications Act 1959 and Obscene Publications Act 1964
- Protection of Children Act 1978 (Section 1)
- Protection from Harassment Act 1997
- The Equality Act 2010
- Regulation of Investigatory Powers Act 2000
- Sexual Offences Act 2003
- EYFS
- Prevent Duty 2023

Contacts for reporting concerns

- Local Designated Officer (LADO) – 0300 123 1650 (option 3) or LADO@surreycc.gov.uk
- EYCS Named Person for allegations against adults working with children and young people - Tel 01372 833895.
- North East Referral Hub– Tel: 0300 123 1610
- Internet Watch Foundation (https://www.iwf.org.uk/) to report illegal images (child sexual abuse material);
- the Child Exploitation and Online Protection centre (CEOP) at https://www.ceop.police.uk/safety-centre/ if worried about online abuse or the way that someone has been communicating online;
- the UK Safer Internet Centre Helpline for Professionals

- Internet Watch Foundation: https://www.iwf.org.uk/
- NSPCC

Further guidance

- Keeping Children Safe in Education
- Online Safety Considerations for Managers
- Education for a Connected World
- childnet.com
- internetmatters.org
- UK Safer Internet Centre
- Education Safeguarding Team on education.safeguarding@surreycc.gov.uk for advice, information and guidance on safeguarding arrangements and practice for settings
- https://help-for-early-years-providers.education.gov.uk/safeguarding-and-welfare/internet-safety
- Children's Media Use and Attitudes report 2023

This policy was adopted by:	Little Fishes Pre-school on 22 April 2026
next review date:	April 2027
Signed on behalf of the provider by	 Alison Carr, Chair of Little Fishes Management Group

Appendix: Little Fishes Acceptable Use Policy

ICT and related technology such as email, the internet and mobile devices are an expected part of our daily working life. This policy is designed to make sure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to read, understand and sign this policy and adhere at all times to its content. If you have any concerns or need any clarification you can talk to the Little Fishes E-safety lead Deborah Johnson.

- ✓ I will comply with the Little Fishes E-safety policy.
- ✓ I understand that using the setting's ICT system for a purpose not permitted by Little Fishes may result in disciplinary or criminal procedures.
- ✓ I will comply with the ICT system security and not disclose any passwords provided to me by the management team.
- ✓ I will only use the setting's email/internet for professional purposes only.
- ✓ I will not install any hardware or software without the permission of the Operations Manager or setting manager.
- ✓ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- ✓ I understand that my use of the internet and other related technologies can be monitored and logged and be made available, if requested as part of any investigation.
- ✓ I will respect copyright and intellectual property rights.
- ✓ I will only take, securely store and use images of children, young people or staff for professional purposes in line with the setting's policy and with written consent of the parent, carer or staff member. I will not distribute images outside the setting without the permission of the parent/carer, member of staff or manager.
- ✓ I will make sure that my online activity both inside and outside the setting will not bring my professional role and the setting's reputation into disrepute.
- ✓ I will support the setting's e-safety policy and help children to be safe and responsible in their use of ICT and related technologies.
- ✓ I will report any incidents of concern regarding children's safety to the e-safety lead/ DSL /Managers.
- ✓ I understand that sanctions for disregarding any of the above will be in line with the setting's disciplinary procedures and serious infringement may be referred to the police.

Signed by: _____ Date: _____