



Internet and E- safety Policy

STATEMENT OF INTENT

Our pre-school wants to create a safe learning environment for children, encompassing all resources available to us.

AIM

Little Fishes Pre-school aims to set out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard adults, children and young people within an early years setting. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate developments within ICT.

IMPLEMENTATION

Our designated e-Safety Lead is **Vicki Walton**. She will take the lead responsibility to ensure that e-Safety is addressed properly.

In order to create a safe learning environment, the setting will:

- Ensure that all members of staff, students, volunteers and visitors are aware of and understand our e-safety policy.
- recognise the importance of e-Safety and understand the setting's duty of care for the safety of the children and staff team
- establish and maintain a safe ICT learning environment within the setting.
- Ensure that any educational material viewed from the internet is screened from beginning to end, prior to being shown to the children, to ensure its suitability
- Take into account that many mobile phones have built-in cameras and will ensure that they are not used to photograph or video children. With this in mind, staff mobile phones will not be used within the setting.
- Request that visitors use their phones only outside the building and store them in a secure place whilst in the setting.
- Store digital photographs on the pre-school computer, which is password protected, until the pre-school ceases to operate. Should this occur then all photographs will be shredded or deleted from the pre-school computer.



- Seek specific parental permission to use photographs of the children taking part in an activity to advertise/promote our pre-school via our website etc. in accordance with the Data Protection Act 1998
- Request verbally, and via a signed document, that parents keep photos and videos for personal use and not to post them on social media sites, such as Facebook.
- ensure that any equipment which holds sensitive or confidential information and leaves the premises is encrypted/password protected
- share any e-safety progress and updates at all staff/committee meetings and ensure that all present understand the link to child protection
- ensure that all staff take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly.
- Advise staff against being connected to any current parents on social media sites
- report any e-Safety incident, concern or misuse of technology by staff, visitors or parents to the e-Safety lead or Manager, including the unacceptable behaviour of others.

INAPPROPRIATE USE

If an employee is believed to have misused the internet or setting network in an illegal, inappropriate or abusive manner, a report must be made to the Manager immediately. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

- MASH team – 0300 126 1000
- Police/CEOP (if appropriate)

In the event of minor or accidental misuse, internal investigations should be initiated and staff disciplinary procedures followed only if appropriate.

Examples of inappropriate use

- Accepting parents as 'friends' on social networking sites if this contradicts the setting's policy
- Behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.



Policies and Procedures

Section 7

Date policy adopted / reviewed 16 June 2016

Signed on behalf of the management committee _____

Name and position of signatory John McCree, Chairman

Policy review date June 2017