



E-Safety – Acceptable Use Policy

This policy is to be used in conjunction with our 'E-Safety – Internet Policy

The policy applies to all employees, volunteers, students and directors. We ensure that visitors are made aware of the expectation that technologies and the internet are used safely and appropriately.

Policy statement:

The purpose of the Acceptable Use Policy is to clearly identify for the whole setting community:

- The steps taken to ensure the E-Safety of children when using the internet and online technologies.
- The setting’s expectations for the behaviour of all users whilst accessing the internet or online technologies within and beyond the setting.
- The setting’s expectations for the behaviour of staff when accessing and using data.

EYFS key themes and commitments:

A Unique Child	Positive Relationships	Enabling Environments	Learning and Development
1.3 Keeping Safe	2.2 Parents as Partners	3.3 The Learning Environment 3.4 The Wider Context	4.4 Areas of Learning and Development

Legal Background:

All adults who come into contact with children in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of all early years’ employees, in relation to use of technologies, feature within the following legislative documents which should be referred to for further information:

- The Children Act 2004
- Working Together to Safeguard Children 2010
- Statutory Framework for the Early Years Foundation 2012
- Safeguarding Vulnerable Groups Act 2009

Staff and Individuals responsibility:

All employees, volunteers and directors must:

- Be familiar with our E-Safety policy and ensure that it is followed at all times.

- Ensure that children are protected and supported in their use of technologies.
- Report any E-Safety incidents, concerns or misuse of technology to the e-Safety lead Ellie Hanna.
- Only use pre-school devices when taking digital images of children.
- Ensure that all electronic communication with parents, carers and other professionals, is only performed on nursery computers. In line with setting protocols. Personal details, such as mobile number, social network details and personal e-mail should not be used or shared.
- Understand that behaviour in their personal lives may impact upon their work with those children if shared online or via social networking sites.
- Not 'friend' any parent/carer of children of current children in the nursery unless they have sought permission from the E - Safety Lead with a valid reason.
- Protect their passwords/personal logins and log-off the network wherever possible when leaving work stations/IPADS unattended.
- Understand that network activity and online communications on setting equipment (both within and outside of the work environment) may be monitored by the E-safety lead.
- Keep their mobile phones in their bags in the office and only use them during lunch breaks away from the nursery. Use only the nursery phone for outings.
- Understand that if they or other colleagues ignore the nursery policies and procedures, that they risk dismissal from their role and possible police involvement if appropriate.
- Given the nature of the role of a director, it may be relevant for manager to communicate with parents, via social media. This is particularly pertinent in the role of promoting nursery events. It is the responsibility of the individual to uphold confidentiality at all times and to act in a professional manner if using social media to promote the nursery or communicate with parents.

This Policy was written by:	Ellie Hanna.
Adapted by:	Katie Tobutt
Read and agreed by:	Little Tinkers Nursery Staff
Date:	October 2022
Review Date:	October 2023