



## 1.9 Online Safety Model

This policy was adopted at the meeting of Little Thetford Acorns Pre-school and Children's Club. Staff failure to comply with this policy may be considered serious enough to result in the induction of disciplinary procedures.

<b>Date of adoption</b>	October 2018
<b>Reviewed</b>	September 2019
<b>Signed (on behalf of the management committee)</b>	
<b>Name of signatory</b>	Kate Hilton
<b>Role of signatory</b>	Chair
<b>This policy will be reviewed</b>	Annually
<b>Date of next review</b>	September 2020

## 1.9 Online Safety Model

### **Safeguarding and Welfare Requirement: Child Protection**

The safeguarding policy and procedures must include an explanation of the action to be taken in the event of an allegation being made against a member of staff, and cover the use of mobile phones and cameras in the setting

#### **Policy statement**

We recognise the exciting opportunities technology offers to staff and children in our setting – however we are also mindful that practitioners have a duty of care to ensure that children are protected from potential harmful online material and that appropriate filtering and monitoring systems are in place.

We encourage adults and children to use a range of technological resources for a wide range of purposes. At the same time, we do all we can to ensure that technology is used appropriately and that children are safeguarded against all risks. While it is not possible to completely eliminate risk, any e-safety concerns that do arise will be dealt with quickly to ensure that children and staff adhere to safe practices and continue to be protected. We will communicate our safe practice in the use of technologies with families and manage any concerns.

This policy applies to everyone- staff, children, parents/carers, visitors and contractors accessing the internet or using technological devices on the premises. The policy is also applicable where staff or individuals have been provided with setting issued devices for use off-site. **We aim to:**

- Raise awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many learning and social benefits
- Maintain a safe and secure online environment for all children in our care.
- Provide safeguarding protocols and rules for acceptable use to guide all users in their use of technology and online experiences
- Ensure all adults are clear about sanctions for misuse of any technologies both within and beyond the early years setting.

#### **Procedures**

- Our designated person (manager/deputy) responsible for co-ordinating action taken to protect children is:

---

#### **Information Communication Technology (ICT) equipment**

- Only ICT equipment belonging to the setting is used by staff and children.
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- All computers have virus protection installed.
- The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.

## **Hardware and provision use**

Where staff have been issued with a device (e.g. Hudl, laptop and emergency mobile) for work purposes, personal use whilst off site is not permitted unless authorised by the manager. These devices should be used by the authorised person only. Setting issued devices only should be used for work purposes and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted. In the case of an outing, all data must be transferred/deleted from the setting's camera/device before leaving the setting.

Personal mobiles and tablets should only be used in the office and be placed in the designated tray. Staff taking photographs or recording with technology not owned by our setting is not allowed.

Online searching and installing/downloading of new programs and applications is restricted to authorised staff members only. Children should not be able to search or install anything on a setting device. All staff have a shared responsibility to ensure that children are supervised when using the internet and related technologies to ensure appropriate and safe use as part of the wider duty of care and responding or reporting promptly issues of concern.

## **Data Storage and Management**

No electronic documents that include children's names or digital images will be transported out of the setting e.g. on a memory stick.

Setting issued devices should not leave the premises unless encrypted. In the case of an outing, all data must be transferred/deleted from the setting's camera/device before leaving the setting.

## **Email**

The setting has central email addresses for all setting related business, including communication with parents/carers:

[Enquiry-littlethetfordacorns@btconnect.com](mailto:Enquiry-littlethetfordacorns@btconnect.com)

[Office-littlethetfordacorns@btconnect.com](mailto:Office-littlethetfordacorns@btconnect.com)

[Manager-littlethetfordacorns@btconnect.com](mailto:Manager-littlethetfordacorns@btconnect.com)

This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.

Staff must not engage in any personal communications (i.e. private email accounts, Whatsapp or via social media) with children who they have a professional responsibility for. This also prohibits contact with children who previously attended the setting.

Staff should not participate in any material that is illegal, obscene and defamatory or that is intended to annoy or intimidate another person or persons.

All emails should stay professional in tone and checked carefully before sending, just as an official letter would be. Care should be taken when forwarding emails from others.

## **Social Networking**

Employees must not access personal blogs/social networking sites on work premises or use the setting's internet systems or email address for their own use, without prior agreement or in accordance with the setting's policy.

The setting does not condone employees writing about their work on social networking sites or web pages. If employees choose to do so, they are expected to follow the rules below:

### **Staff must not:**

- disclose any information that is confidential to the setting or any third party or disclose personal data or information about any individual child, colleague or service user, which could be in breach of the General Data Protection Regulations and Data Protection 2018
- disclose the name of the setting or allow it to be identified by any details at all. This includes posting photos of children and young people, the premises or events with work colleagues.
- link their own blogs/personal web pages to the setting's website.
- make defamatory remarks about the setting, colleagues or service users.
- misrepresent the setting by posting false or inaccurate statements.

**Communication with children and young people, by whatever method, should always take place within clear and explicit professional boundaries. Staff should avoid any misinterpretation of their motives or any behaviour that could be construed as grooming.**

Staff should not: send social networking site 'friend requests' to, or accept them from, children, young people or parents who use the setting.

Failure to adhere to the rules and guidelines in this policy may be considered misconduct and could lead to disciplinary and /or criminal investigations.

**Remember that anything posted online could end up in the public domain to be read by children, parents or even future employers – so be careful what you post and who you post it to. For example, posting explicit pictures of yourself could damage your reputation and that of your profession and organisation. Parents and employers may also question your suitability to care for children.**

### **Use and/or distribution of inappropriate images**

- Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately, the Safeguarding Children and Child Protection policy, in relation to allegations against staff and/or responding to suspicions of abuse, is followed
- Staff are aware that grooming children and young people online is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).

## Setting social media sites

Setting social networking sites containing information about children attending the setting must be “closed” i.e. the users of the site are accepted and monitored by the manager/administrator. No staff, families or children’s personal information will be accessible by users of the site and the manager/administrator will ensure that users’ profiles are kept private. The manager/administrator will moderate all postings to the site; they will view and quality assure these before they appear, for example, to ensure they do not reveal personal information.

## Electronic learning journals for recording children’s progress

- Managers seek permission from the senior management team prior to using any online learning journal. A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
- Staff adhere to the guidance provided with the system at all times.

## Sanctions

Misuse of technology or the internet may result in:

- the logging of an incident
- disciplinary action
- reporting of any illegal or incongruous activities to the appropriate authorities
- allegations process being followed

Other relevant policies and guidance

- NSPCC and CEOP *Keeping Children Safe Online* training: [www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/](http://www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/)

## Guidance for settings on the use of images and technological devices

### Useful contacts

Education Child Protection Service	<a href="mailto:ecps.general@cambridgeshire.gov.uk">ecps.general@cambridgeshire.gov.uk</a>
------------------------------------	--

Early Years Safeguarding Manager	01223 714760
----------------------------------	--------------

Local Authority Designated Officer (LADO)	01223 727967
---	--------------

## Other useful Pre-school Learning Alliance publications

Safeguarding Children (2013)

Employee Handbook (2012)