




# E-Safety Policy

For the Early Years Staff, Children and Parents, Nursery and Reception Classes

<b>Lead author/initiator(s):</b>	Laura Fielding
<b>Next Review Date:</b>	July 2023
<b>Version No:</b>	1
<b>Ratified by:</b>	Spring Meadow Infant and Nursery School Local Governing Body
<b>Date Ratified:</b>	
<b>Signed :</b>	
<b>Review Timetable:</b>	Annually
<b>Purpose of Document:</b>	To ensure that technology is used appropriately and that children are safeguarded against all risks where possible

## **Contents:**

Introductory Statement

1. Scope of the Policy
2. A Secure Infrastructure
3. Hardware Provision and Use
4. Mobile Technology
5. Data Storage and Management
6. Email
7. Social Networking
8. Photographs and Videos
9. Sanctions
10. References and Links

## **Introductory Statement**

We recognise the exciting opportunities technology offers to staff and children in Spring Meadows Early Years' provision and have invested in age appropriate resources to support this belief. While recognising the benefits we are also mindful that practitioners have a duty of care to ensure that children are protected from potential harm both within and beyond the physical and virtual boundaries of our setting.

To reflect our belief that when used appropriately and safely, technology can support learning, 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 and in line with Cambridgeshire safeguarding directives 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.

### **1. Scope of the Policy**

This policy applies to everyone- staff, children, parents/carers, visitors and contractors accessing the internet or using technological devices on the premises. This includes the use of personal devices such as mobile phones or iPads/tablets which are brought into the setting. 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 educational and social benefits and therefore the need to safeguard against misuse
- 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.
- Develop a set of AUP's to set out the roles, responsibilities and procedures to govern the acceptable use of all online technologies with the aim of safeguarding children, young people and adults from harm.

## **2. A Secure Infrastructure**

A safe and secure internet access provision through the local authority ensures internet enabled devices minimise the risk of exposure to inappropriate material.

The ICT infrastructure in the setting is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN), CPSN, and the Local Authority's Education ICT Service. E2BN's Protex web filtering system received full Becta (British Educational Communications and Technology Agency) accreditation in 2007 by blocking over 90% of all inappropriate material. Age appropriate content filtering is in place across the setting, ensuring that staff and children receive different levels of filtered internet access in line with user requirements (e.g. Youtube at staff level but blocked to children).

Adults need to be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Permission to access the secure wireless network will need to be granted by a member of the leadership team.

The school employs a number of strategies in order to maximise the opportunities offered by technology and to reduce the risks associated with the use of the internet and all fixed and mobile technologies. These are:

## **3. Hardware Provision and Use**

Where staff have been issued with a device (e.g. setting laptop) for work purposes, personal use whilst off site is not permitted unless authorised by the provider/manager. The settings laptop/devices should be used by the authorised person only.

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.

Software or apps used must be from a pre-approved selection checked and agreed by Matt Courtman and the Head Teacher

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

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.

#### **4. Mobile Technology**

The use of mobile phones by staff in any of the learning spaces either outside or during contact times, or in professional meetings, is strictly prohibited unless given permission from a member of the leadership team. Personal mobile phones and cameras should only be used outside of working hours and never whilst children are present.

Applications (apps) targeted specifically at Early Years Practitioners and settings which allow staff to track and share a child's learning journey online with parents and carers, have considerable benefits, including improved levels of engagement with parents and a reduction in paperwork, but permission from the Head teacher must be given before using such tools.

Personal staff mobile phones or devices (e.g. iPad or iPhone) should not be used for any apps which record and store children's personal details, attainment or photographs. Only setting issued devices may be used for such activities, ensuring that any devices used are appropriately encrypted if taken off site.

Personal mobile phones must never be used to contact children or their families, nor should they be used to take videos or photographs of children. In circumstances such as outings and off site visits, staff will agree with their manager the appropriate use of personal mobile phones in the event of an emergency.

Where there is a suspicion that the material on a mobile phone may be unsuitable and may constitute evidence relating to a criminal offence, the 'Allegations of Abuse' process will be followed (please refer to the setting's 'Safeguarding and Child Protection Policy').

#### **5. Data Storage and Management**

No electronic documents that include children's names or digital images will be transported out of the centre e.g. on Fobs. Central Hosting can be used by all staff who need to access electronic work from home.

Only the Account Operator (usually the Office Manager) can manage the user accounts on Centrally Hosted emails and MIS systems. All activity in this user tool will be logged and kept for a minimum of one month in case of incident.

#### **6. Email**

In line with Local Authority practice and guidance, the setting provides all staff with access to a professional email account to use for all work related business, including communication with

parents/carers. 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. via hotmail or yahoo accounts etc.) with children who they have a professional responsibility for. This also prohibits contact with former pupils outside of authorised setting email channels.

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.

## **7. Social Networking**

Due to the public nature of social networking and the inability to keep content truly private, we take great care in the management and use of such sites. Best practice guidance states that 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 Data Protection Act.
- 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
- 'Friend' parents without the explicit permission of those parents and should ensure all privacy settings are set to maximum and checked regularly.

## **8. Photographs and Video**

Digital photographs and videos are an important part of the learning experience in early years settings and, as such, staff have a responsibility to ensure that they not only educate children about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and children about the use of digital imagery and videos.

The Data Protection Act 2018 affects the use of photography. An image of a child is personal data and it is, therefore, a requirement under the Act that consent is obtained from the parent/carer of a child for any images made such as those used for setting websites, observations, outings and events or other purposes. It is also important to take into account the wishes of the child, remembering that some children do not wish to have their photograph taken.

Written consent must be obtained from parents or carers before photographs or videos of young people will be taken or used within the setting, including displays, learning journeys, setting website and other marketing materials.

Avoid using children's first and last name nor use children's names in image files if published on the web.

Only technology owned by the school will be used on the premises and on centre visits. This includes mobile devices for everyday use and, in case of emergency, a mobile phone is provided. Staff taking photographs or video with technology not owned by our centre is specifically not allowed. Visitors will need to seek permission from the head of centre should they want to take photographs of children from the centre. However, in exceptional circumstances, such as equipment shortages, permission may be granted by the Provider/Manager for use of personal equipment for setting related photographs or videos, provided that there is an agreed timescale for transfer and deletion of the image from the staff member's device.

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

## **9. Sanctions**

Misuse of technology or the internet may result in

- the logging of an incident
- disciplinary action at the discretion of the Head Teacher
- reporting of any illegal or incongruous activities to the appropriate authorities

Sign to say that you have read and understood and will take all appropriate actions in line with this policy.

\_\_\_\_\_ Dated:  
Member of staff

## **10. References and Links**

E-Safety Incident Guidance and Flowchart

[http://www.cambslscb.org.uk/prof\\_e\\_safety.html](http://www.cambslscb.org.uk/prof_e_safety.html)

Cambridgeshire Local Safeguarding Children's Board

<http://www.cambslscb.org.uk/>

Cambridgeshire County Council Safeguarding in Early Years

<http://www.cambridgeshire.gov.uk/childrenandfamilies/children-services/workingwithpartners/earlyyearsandchildcare/curriculum/eychildprotection.htm>

Safer Children in a Digital World

<http://dera.ioe.ac.uk/7332/1/Final%20Report%20Bookmarked.pdf>

Zero to Eight Report

[http://eprints.lse.ac.uk/52630/1/Zero to eight.pdf](http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf)

Plymouth Early Years Toolkit

<http://www.plymouth.gov.uk/homepage/education/earlyyearsandchildcare/onlinesafetytoolkit.htm>