Registered Charity # 1203754

Online Safety Policy

Introduction

Houghton and Wyton Pre-school recognises that online technology and digital communication are increasingly a part of everyday life. While children in our setting do not independently access the internet, this policy ensures that all online and digital activity by staff, volunteers, and the setting as a whole complies with safeguarding, data protection, and professional standards.

This policy should be read in conjunction with the Use of Mobile Phones, Cameras, and Technological Devices Policy.

Aim

To ensure the safe, responsible, and lawful use of all digital devices, online systems, and communication channels used within or on behalf of the setting.

Objectives

We will:

- Protect children from online risks such as grooming, exposure to inappropriate content, and unauthorised sharing of personal information
- Ensure that staff and volunteers model safe and respectful digital conduct
- Manage the use of devices, photographs, and digital records securely
- Support families in promoting online safety at home

Roles and Responsibilities

- **Online Safety Lead**: Monitors digital safety, device use, and oversees training, reporting, and response to incidents
- **Staff and Volunteers**: Follow this policy in all use of phones, emails, social media, and data
- **Parents/Carers**: Are informed of online safety practices and asked to support safe image-sharing and digital conduct at home

Implementation Procedures

1. Use of Technology in the Setting

- Children do not access the internet directly
- Staff may use setting devices (tablets, laptops) for:
  - Recording observations
  - Secure access to Famly and digital planning tools
- Devices must be password-protected and never left unattended while logged in

2. Use of Personal Devices and Mobile Phones

- Staff and visitors must store personal mobile phones securely during sessions
- Phones must not be used for taking photographs or storing children's data
- Any breach is recorded and dealt with in line with the Safeguarding and Staff Conduct policies

3. Photography and Use of Images

- Photographs are only taken with setting devices (not personal phones)
- Written consent is obtained from parents for photo use
- Images are:
  - Stored securely
  - Used for learning journals, displays, or promotion only with permission
  - Never posted on public social media without prior written consent

4. Communication and Email Use

- All communication with families must:

  - Be professional and respectful
  - Be via official channels (Famly, setting email, or face-to-face)
- Staff may not use personal accounts for work communication
- DSL's and SENCOs will be provided an appropriate professional email address to receive and send confidential information regarding the care and wellbeing of a child. DSL's and SENCOs will provide an alternative, confidential email address in times od leave, to ensure a timely response.

5. Social Media and Public Conduct

Staff must:

- Not identify children or families from the setting on personal social media
- Not post photos of children from the setting (including their own children with others)
- Not make negative or defamatory comments about the setting, staff, or families
- Use privacy settings on all personal platforms and exercise professional judgment

6. Online Safety Education and Parent Partnership

- We provide age-appropriate activities about privacy, respect, and safety in the digital world
- We share tips and resources with families about staying safe online at home (e.g. screen time, YouTube Kids, privacy settings)

7. Incident Reporting and Breaches

- Online safety incidents (e.g. inappropriate content, data breaches) are reported to the Manager immediately
- Incidents are recorded and escalated using the Safeguarding Policy or Data Breach procedure where necessary
- The setting may restrict or remove device access if a risk is identified

Monitoring and Review

This policy is reviewed annually by the Online Safety Lead and Board of Trustees or sooner if legislation or best practice changes. Digital safety is monitored through supervision and incident logs. Device use and image storage are periodically reviewed to ensure compliance with this policy.

Legislation and Guidance

- Statutory Framework for the EYFS (2023) – Section 3.4
- UK Council for Internet Safety Guidance (2019)
- Data Protection Act 2018 and UK GDPR
- Working Together to Safeguard Children (2018)
- Keeping Children Safe in Education (for reference)

Acknowledgment

All staff, trustees, volunteers, and visitors must follow this policy. By doing so, they help create a safe and respectful digital environment for all children and adults at our setting.