E-Safety Policy

At Pippins we recognise the value that communication and technology plays in the learning and development of children whilst allowing children to discover, connect and create.

We acknowledge that there are potential risks involved and therefore follow this policy to ensure the safety of Practitioners, children, parents and visitors to the Preschool.

The designated practitioner responsible for ensuring ICT equipment is safe and fit for purpose is **Alice Redman**.

Overview of Policy
As a setting we aim to promote Online safety by promoting the protection of children and young people and striving to avoid exposing them to unwanted consequences. We are aware that there are the 4 C's of risk that children can be exposed to online, these are:

- Content – such as inappropriate content, exposure to extreme views and behaviour promoting violence
- Contact – such as Grooming, Identity Theft or Online Bullying
- Commercialism – such as adverts, tricking people into payments they don't expect
- Conduct – such as materials effecting people's Mental Health and Wellbeing

The narrative below shows how as a setting we strive to remove these dangers as children access or interact with online/e-materials.

Photography
Parents' permission is actively sought to use the photos/video of their children for the purpose of displays, publicity (both on Facebook and on our Website) and on our BabysDays learning journey system. We also ask parental permission for their child to be photographed by a professional photographer or by parents for special events.

Only photos taken by educators with a setting camera, ipad or video camera will be used in the setting or on the website/Facebook.

If there are outside photographers attending the setting for any reason other than that of school photos, we will notify parents and ask for their permission separately for the child to be photographed.

When an event takes place such as Christmas Party or fundraising day where other parents may take photos, we will notify parents of this occurrence in advance. We will however highlight the feelings of other parents over the usage of photos on social media if they contain other people's children.

We will discuss with parents any concerns they have with any of the photography occurring in and out of the setting. We hope that an understanding can be reached in all situations. In situations where photos are used on Social Media or on our Website, children will not be named.

Use of Mobile Phones/Smart Watches
Educators will never take photos on their own personal cameras or mobile phones. Mobile phones are kept out of the play areas along with personal belongings. Parents and visitors will

be asked to place their phone in the office upon arrival and not to take phone calls on the setting floor.

Whilst not encouraged educators can use the setting Wifi on private devices such as laptops and mobile phones.

Due to the potential of video and audio recording functions, educators are prohibited from wearing smart watches that have photo facilities whilst at work.

Children are not permitted to bring mobile phones into the setting, if they do these will be removed from them and stored appropriately till they can be passed to a grownup.

Social Media
Pippins Pre-School has an active Facebook account. This page shall only be used to post notices and updates of activities within the setting. Only photos of children whose parents have given consent will appear on our Facebook page. If photos are used there will be no mention of names alongside photos.

Any communication or content practitioners/committee members publish that causes damage to the setting or any of its employees, children or families may constitute misconduct or gross misconduct and could lead to dismissal. Confidentiality by practitioners is ensured by a confidentiality agreement.

All staff and Committee members should bear in mind that information they share through social networking applications, even though they are in a private spaces, are still subject to copyright, data protection and freedom of information legislation, safeguarding vulnerable groups act 2006 and other legislation.

Educators should not encourage parents or children as friends on social networking sites.

Use of Video Technology
Within our setting we have access to laptops, smart doorbell and a home security camera (in our Sensory Cabin) all which incorporate video and audio technology. We use these to ensure the safeguarding of our children and our staff.

The information recorded on these devices is stored securely and deleted when appropriate - see GDPR schedule.

For additional protection all preschool laptops are equipped with camera covers.

Visitors to the Sensory Cabin will be asked if they wish for the recording device to be turned off. Additional staff will be asked to enter for the duration of the meeting if appropriate.

Internet Use
Children's access to the internet will be supervised and they will only have access to sites specifically chosen by us . Educators will also pay due attention to the length of time children are accessing screens in the setting following Government guidelines released in March 2026.

All inappropriate/offensive material such as those that site bullying, racism or discrimination will be reported by Practitioners to the **Internet Watch Foundation (IWF)** www.IWF.org.uk

Suspicions that an adult is attempting to make inappropriate contact with a child online will be reported to The National Crime Agencies, **Child Exploitation and Online Protection Centre (CEOP)** at www.ceop.police.uk.

If Educators become aware that a child has become a victim of cyberbullying they discuss this with their parents and refer to sources of help such as the NSPCC www.nspcc.org.uk or child line 0800 1111 or www.childline.org.uk

Additional Protection
All laptops are equipped with Anti-Virus software.

The designated person ensures that safety settings are set so that inappropriate materials are not accessed. Tablets and other equipment are set up to use Kiddle and Youtube kids.

E-Safety
Children that attend the Pre-School and Wrap Around Care are spoken to about e-safety in an age appropriate way. We will engage national initiatives with the children regarding this subject.

Other Technology used
A list of other technology used in the setting; Mobile phone (for use in emergencies or on outings), Alexa, CD players, Walkie Talkies, Switch and ChromeCast but this list is not exhaustive.

Technology outside the setting
All Educators using personal computers at home for the purposes of work are made aware that they should be protected by secure passwords that are changed regularly and have recognised anti-virus software installed.

Emails
The Pre-School has designated email addresses for professional correspondence that are password protected and changed regularly.

Educators send personal information by secure email.

Storing of Documents
As a setting we hold information on encrypted memory sticks, Babysdays and a secure cloud. All Laptops are also password protected. For full information on what personal data is kept and how it is stored please see our GDPR Schedule.

Tablets used within the setting are locked away securely at the end of each day.

In the event that inappropriate use of technology is identified then our Local Authority Designated Officer (LADO) will be contacted immediately. We will follow the guidance of the LADO.

Further guidance for parents:
NSPCC and CEOP - 'Keeping children safe online'
https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Government Documentation - https://www.gov.uk/government/publications/coronavirus-covid-19-keeping-children-safe-online

Screen-time guidance for Setting and Parents
New screen time guidance for parents of under-5s - GOV.UK

This policy was adopted on:.....

Signed on behalf of the setting……..

Date of next review:.....