E-Safety Policy

This policy will be reviewed on an annual basis

Aim;

Pippins has a duty to ensure that children are protected from potential harm, both within and beyond the learning environment. To ensure children are offered the opportunities by advances in information and communications technology (ICT), while ensuring children are safeguarded and protected from potential harm, by implementing procedures and information to help keep children safe online.

Actions;

Mobile Phones and Mobile technology

Pippins pre-school and nursery have policies and procedures in place with regard to the use of mobile phones and electronic devices with imaging and sharing capabilities i.e. ipad's, smart watches, laptops, cameras in the setting and on visits etc.

- All staff, students, volunteers and visitors are discouraged from bringing their mobiles phones or electronic devices into the setting. If the staff member, student, volunteer or visitor feels it is essential to bring their phone/electronic device to the setting it will be handed into the office upon arrival, passing it through one of the allocated slots in the glassed window to the office. Their mobile phone will then be locked away securely, with only management and the clerical assistant having access.
- Staff, students, volunteers and visitors are encouraged to use their mobile phone away from Pippins premises, however are able to check/use their phone in the office in the presence a member of the management team. If they wish to access their phone during their designated break or at the end of their shift, they can receive it back through the glass window in the front foyer and then exit the building through the front door. The staff member, students, volunteers and visitors can then use their phone once outside and away from the building.
- All of the above also applies to any technology which has an imagining facility built into the system.
- Management and the clerical assistant are only permitted to have access to their phone in the office for work purposes such as organising staffing.
- Smart watches are permitted but must be on 'silent' and 'do not disturb' mode as well as not connected to the Pippins wifi. Should staff be seen to be using these for purposes other than a watch, our disciplinary procedure will be followed.
- Should a professional arrive needing access to their laptop to write notes or discuss a document stored on the device, will be permitted and our safeguarding, and visitors policy will be followed (not leaving the visitor alone in the setting).
- Early years educators, students, volunteers and visitors must inform their emergency contacts and anyone likely to contact them during working hours on Pippins land line telephone number 01363 772474, and in when necessary can make an external call.
- We have two designated mobile phones that are taken on trips and only used in the event of an emergency. These phones are kept locked in the office and only are put in our 'trips bag' when leaving the setting, where they are kept for the duration of the trip unless needed. When arriving back to the setting the phones are given back into the office,
- Staff are aware of e-safety issues and receive regular up-to-date e-safety training.
- The use of the internet by employees of Pippins Pre-School and Nursery is permitted where such use supports the goals and objectives of the business.
- Staff will incorporate e-safety in to the planning curriculum.

- Staff must:-
  - Comply with current legislation
  - Use the internet in an acceptable way inside and outside of work
  - Do not create unnecessary business risk to the company by their misuse of the internet including typed posts or photo images on social networking sites such as Instagram, Twitter, Facebook etc

Whilst we cannot govern employee's use of the internet outside of work, we strongly recommend staff comply with the above ensuring they safeguard themselves.

Risks

Experts believe that by raising awareness of online risks at an early age, children will be better protected as they grow up.

Staff recognise the following risks: -

- Prolonged exposure to online technologies, particularly from an early age
- Exposure to illegal, inappropriate or harmful content
- Grooming
- Cyberbullying
- Making, taking and distribution of illegal images and inappropriate messages.
- Physical, sexual and emotional abuse
- Identity theft
- Privacy issues
- Addiction to gaming or gambling
- Pressure from the media and targeted advertising
- Theft and fraud from activities such as phishing, viruses, malware, etc
- Damage to professional online reputation through personal online behaviour.

Company-owned information held on third-party websites

Any information referring to Pippins Pre-school and nursery or information regarding a child, parent or families past and present connected to Pippins Pre-school and nursery which is displayed on third party websites remains the property of Pippins Pre-school and nursery.

Monitoring

Pippins will manage the following risks by educating all staff and through monitoring.

Pippins Pre-school and nursery accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

- Reasonable precautions will be taken to protect users and is essential practice for Early Years educators.
- All of the company's internet related resources are provided for business purposes. Pippins maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.
- Staff will ensure the content is filtered and age appropriate.
- Use a recognised internet provider.
- Use antivirus software which is updated.
- Use egress when sending confidential e-mails.
- Computers/laptops/iPads to be logged off when not in use and are password protected. .

Sanctions
Any employee failing to comply with the policy, will follow Pippins disciplinary procedures.

For clarification purposes the following are examples of misuse of technology and a breach of policy and will be deemed as gross misconduct: -

- Visiting internet sites that contain obscene, offensive, inappropriate images or otherwise illegal material.
- Using Pippins computers to perpetrate any form of fraud, or software, film or music piracy.
- Using the internet to display or to send offensive or harassing materials that belong to third parties, unless this download is covered or permitted under a commercial agreement or other such license.
- Accessing into unauthorised areas
- Publishing defamatory and/or knowingly false material about Pippins Pre-School and nursery, your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of malicious software into the corporate network.

Reporting
All staff will report any E-safety breach to management and follow our Whistleblowing Policy.

Agreement
All company employees, contractors, volunteers, students or temporary staff are required to sign the agreement confirming their understanding and acceptance of this policy.

1. **I confirm I have read and understood Pippins Pre-school and nursery E-Safety Policy.**
2. **I agree to store my phone/electronic device away in the designated safe.**

Name .....

Signature .....

Date .....

This policy was adopted at a meeting of Pippins Pre-school and nursery

Held on Thursday 19th October 2023

Signed on behalf of the Management Trustee Director

Role of signatory (e.g. chair etc.) Chair

Commenced 2010- Revised 20.10.2021, 1.2.22, 07.03.2024