PEWSHAM PRESCHOOL LTD POLICIES AND PROCEDURES

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.

1.6 Online Safety (including mobile phones, cameras and social networking)

Policy statement

We take steps to ensure that there are effective procedures in place to protect children, young people, and vulnerable adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting.

The settings Designated Safegaurding Lead is responsible for co-ordinating action taken to protect children with regards to ICT and ensures:

- Only ICT equipment belonging to the setting is used by staff and children when in the setting.
- The designated person is responsible for ensuring the 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.

Procedures

Mobile phones – adults

- Personal mobile phones and other smart technology, such as smart watches with built in cameras, belonging to our staff and volunteers are not used on the premises during working hours.
- Smart watches that do not have a camera facility may be permitted once they have been checked by the setting manager. Staff must ensure that notification settings are set to off to prevent interruptions during working hours.
- At the beginning of each individual's shift, personal mobile phones/smart technology devices are stored in the office and staff will only have access to these when they are on their breaks and not in contact with the children.
- In the event of an emergency, personal mobile phones may be used in privacy, where there are no children present, with permission from the manager.
- Our staff and volunteers ensure that the work telephone number is known to immediate family and other people who need to contact them in an emergency.
- If our members of staff or volunteers take their own mobile phones on outings, for use in the case of an emergency, they must not make or receive personal calls as this will distract them.
- Our staff and volunteers will not use their personal mobile phones or other smart technology for taking photographs of children on outings.
- Parents and visitors are requested not to use their mobile phones or other smart technology whilst on the premises. We make an exception if a visitor's company or organisation operates a lone working policy that requires contact with their office periodically throughout the day. Visitors will be advised of a quiet space where they can use their mobile phone, where there are no children present.

Mobile phones – children

- Children are not permitted to bring mobile phones or other ICT devices into the setting. If a child is found to have one it will be removed from them and placed in the office until the end of the session.

Cameras and videos

- Our staff and volunteers must not bring their own cameras or video recorders into the setting.
- Photographs and recordings of children are only taken for valid reasons, i.e. to record their learning and development, or for displays within the setting.
- Photographs or recordings of children are only taken on equipment belonging to the setting.
- Camera and video use is monitored by our manager.
- Where parents request permission to photograph or record their own children at special events, permission will first be gained from all parents for their children to be included.
- Photographs and recordings of children are only taken of children if parents provide written permission to do so found on the individual child's Registration Form.

Tapestry

. See Online Journal Policy 10.12

Safe Online Behaviour/Social Contact

- All staff and volunteers must ensure that social network sites that they join, and hold information available publicly about them, is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves or the preschool if they are published outside of the site.
- Staff are advised to manage their personal security settings to ensure that their information is only available to people they chose to share information with.
- Staff and volunteers will not make a friend, on social networking, of a child or young person associated with Pewsham Preschool Ltd in anyway. Staff and volunteers will not accept an invitation from a child or young person, and where this has been requested they should inform their manager who will decide whether to discuss with the child's parent/carer.
- Staff should not befriend parents or children on any social media site, such as Facebook, unless they already have a relationship with the family before the child starts at preschool. Such friendships should be disclosed to the management
- Staff and volunteers consider confidentiality at all times and must not use any social networking site to discuss or give information about themselves, their employer, their colleagues or children and families of Pewsham Preschool Ltd.
- Formal action will be taken against any member of staff or volunteer who fails to give due regard to the potential of defamation of character about other employees, volunteers or children and families of Pewsham Preschool Ltd.
- Staff and volunteers will comply with the requirements of equalities legislation in their on-line communications. Should a member of staff post derogatory remarks or offensive comments on-line, or engage in on-line activities which could reflect negatively on their professionalism, they will be reported to the Designated Officer in the Local Authority who will consider their suitability to work with children.
- Adults should report any concerns or breaches to the settings designated safeguarding officer.

Protection of personal information/Social Contact

- Staff and volunteers will not share their personal phone numbers with parents and will not use personal devises to make contact with parents of children attending Pewsham Preschool Ltd.
- Staff and volunteers will not share personal email addresses with parents.
- Staff and volunteers will not share the work log-ins or passwords with other people.

Access to inappropriate images and internet usage

- Children do not normally have access to the internet and never have unsupervised access.
- The designated safeguarding lead has overall responsibility for ensuring that risk assessment in relation to online safety are completed.
- If a second hand computer is purchased or donated to the setting we will ensure that no inappropriate material is stored on it before the children use it.
- All computers or ipads used by children are located in an area clearly visible to staff and the ipads have had parental controls added to them to prevent children accessing inappropriate material.
- Children are not allowed access to social networking sites.
- Staff must report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.
- There are no circumstances that will justify adults possessing indecent images of children. Any adult who access or possesses links to such websites will be viewed as a significant and potential threat to children and will be immediately reported to the police and local authority Designated Officer.
- Staff and volunteers will not use any equipment belonging to Pewsham Preschool Ltd to access any adult pornography; neither should personal equipment containing these images be brought into the workplace. Failure to comply with this will raise serious concerns about the suitability of the adult to work with children.
- Staff and volunteers will ensure that children are not exposed to any inappropriate images whilst using ICT equipment in the setting by ensuring appropriate controls are in place.

Email

- Children are not permitted to use email in the setting. Parents and staff are not normally permitted to use setting equipment to access personal emails.
- Staff do not access personal or work emails whilst supervising children.

Cyberbulling

- Cyberbullying is defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power over them'.
- Staff and volunteers are reminded of the importance of complying with this policy to help protect them from this type of abuse.
- Staff and volunteers are aware that any accusation of cyberbullying is considered a disciplinary matter and may lead to criminal investigation and conviction. This is regardless of whether the behaviour has occurred within or outside of preschool, or on preschool or personal equipment.
- All staff and volunteers are encouraged to report all incidents of cyber bullying to their line manager. All incidents will be taken seriously and dealt with accordingly. Records will be kept of the abuse, such as texts, website or instant messages, texts or emails. They should not be deleted and where possible screen prints of messages or websites should be taken and clearly recorded with time and date.
- It is the choice of the individual being bullied whether the incident is reported to the police.

Legislation Framework:

Computer misuse act 1990

Data protections act 1998

Freedom of information 2000

Communications act 2003

Malicious communications act 1998

Criminal justice and public order act 1994

Racial and religious hatred act 2006

Protection from harassment act 1997

Protection of Children’s act 1978

Sexual offences act 2003

Public order act 1986

Obscene publication s act 1959 and 1964

Human rights act 1998