

**Information**

**Security Policy**

Setting Manager: Jane Johnson

Business Manager: Debbie Hoddinott

Policy Approved by: Aston-on-Trent Pre-School Committee Date: March 2024

Policy reviewed by: Date:

Policy reviewed by: Date:

Policy reviewed by: Date:

**Information Security Policy**

**Online Safety**This guidance refers to all electronic devices able to access the internet, take photos or record videos, make or receive calls, send messages and the ability to share information of any other form outside of Preschool. This includes digital cameras, mobile telephones, tablets and any recording devices including smartwatches. As technology moves forward, there are an increasing amount of devices technically capable of sharing private information. As such, this policy will continue to adapt to include all devices we deem important to ensure the safety of our children and staff.

It is important that children and young people receive consistent messages about the safe use of technology and are able to recognise and manage the risks posed in both the real and the virtual world.

Terms such as ‘e-safety’, ‘online’, ‘communication technologies’ and ‘digital technologies’ refer to fixed and mobile technologies that adults and children may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks. The issues are:

* Content – being exposed to illegal, inappropriate or harmful material
* Contact – being subjected to harmful online interaction with other users
* Conduct – personal online behaviour that increases the likelihood of, or causes, harm

**ICT Equipment**

* The setting manager ensures that all computers have up-to-date virus protection installed.
* Tablets are only used for the purposes of observation, assessment and planning, and to take photographs for individual children’s learning journeys.
* Tablets remain on the premises and are stored securely at all times when not in use.
* Children never have unsupervised access to the internet.
* The setting manager ensures that risk assessments in relation to e-safety are completed.
* Only reputable sites with a focus on early learning are used (e.g. CBeebies).
* Video sharing sites such as YouTube are not accessed due to the risk of inappropriate content.
* Children are taught the following stay safe principles in an age-appropriate way:
* only go online with a grown up
* be kind online and keep information about me safely
* only press buttons on the internet to things I understand
* tell a grown up if something makes me unhappy on the internet
* Staff support children’s resilience in relation to issues they may face online, and address issues such as staying safe, appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
* All computers for use by children are sited in an area clearly visible to staff.
* Staff 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](http://www.iwf.org.uk/).
* The setting manager ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

**Mobile Telephones (and internet enabled devices)**  
We understand that our staff have personal commitments that mean they may need to be contactable by phone during the session. Pre-school has a landline and staff are advised that they can be contacted on this number in an emergency.

* Staff are allowed access to their mobile telephone during Pre-school opening hours only during breaks.
* Personal mobiles may be used off the premises or in a safe place e,g. staff room. The setting manager completes a risk assessment for where they can be used safely.
* In an emergency, personal mobile phones may be used in areas such as the hallway, if appropriate, and at the managers discretion.
* Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.
* Members of staff do not use personal equipment to take photographs of children.
* Parents and visitors are asked not use their mobile phones on the premises. There is an exception if a visitor’s company/organisation operates a policy that requires contact with their office periodically throughout the day. Visitors are advised of a private space where they can use their mobile.

**Cameras and Video Recording Equipment**

* Members of staff do not bring their own cameras or video recorders to the setting.
* Photographs/recordings of children are only taken for valid reasons, e.g. to record learning and development, or for displays, and are only taken on equipment belonging to the setting.
* Camera and video use is monitored by the setting manager.
* Photographs/recordings of children are only made if relevant permissions are in place.
* If photographs are used for publicity, parental consent is gained and safeguarding risks minimised, e.g. children may be identified if photographed in a sweatshirt with the name of their setting on it.

**Smart Watches**

* Smart Watches can be worn by staff, but must be either turned off completely or have the Wifi and Bluetooth disabled during working hours. This does not include breaks where Smart Watches may be used off the premises or in a safe place e,g, staff room. The setting manager completes a risk assessment for where they can be used safely.
* Smart Watches may not be used to access photos or videos while on Pre-school outings.

**Voice Assistant Devices & AI Software Assistants**

* Parents/Carers are made aware of the device being used the the setting.
* The device is used under supervision at all times.
* The device has the appropriate age-related security settings enabled.
* Children are not permitted to share any personal information with the device, for example, their name, age or address information.
* The device is switched off at the mains power when not in use.
* The device has all voice recordings deleted daily after use.
* The device is governed by an App on a Pre-school mobile telephone and is the responsibility of the Pre-school manager.

**Use of Social Media**

We feel that guidelines are necessary to ensure that staff understand the proper practices when using and accessing social networking sites. This is to protect the children, parents and other staff, and to guard   
Pre-school’s and your personal reputations.

The policy states that staff members are allowed to use any social networking site as long as they follow these guidelines, regarding the impact social networking has on the Pre-school. Failure to comply may be an invasion of privacy and may infringe our Data Protection Policy.

Guidelines include:

* Staff must not mention any of the children or staff from pre-school on their online profiles.
* Staff must avoid naming Pre-school or writing indirect suggestive comments about pre-school on their social networking sites e.g. ‘I’ve had a bad day at work’
* Staff must not publish photos of children, parents or other staff in pre-school on their profiles.
* Staff must not go on social networking sites whilst in pre-school.
* Staff must understand how to manage their security settings to ensure that their information is only available to friends. This can help to prevent accidental breaches of this policy.
* Staff are aware that comments or photographs online may be accessible to anyone and should use their judgement before posting.
* Staff are aware that images, such as those on Snapchat may still be accessed by others and a permanent record of them made, for example, by taking a screenshot of the image with a mobile phone.
* Staff observe confidentiality and refrain from discussing any issues relating to work.
* Staff do not share information they would not want children, parents or colleagues to view.
* Staff report any concerns or breaches to the designated person in their setting.
* In order to maintain professional boundaries, staff will not accept friendship requests or engage in personal communication, including on social networking sites, with children and parents/carers with whom they act in a professional capacity. There may be occasions when the practitioner and family are friendly prior to the child coming to the setting. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed.

**Use and distribution of inappropriate images**Staff are aware that it is an offence to distribute indecent images and that it is an offence to groom children online. In the event of a concern that a colleague is behaving inappropriately, staff advise the designated person who follows the procedures in our *Allegations Against Staff, Volunteers or Agency Staff Policy* and our *Child Protection and Safeguarding Policy*.

**Cyber Bullying**If staff become aware that a child is the victim of cyberbullying at home or elsewhere, they discuss this with the parents and refer them to help, such as: NSPCC Tel: 0808 800 5000 [www.nspcc.org.uk](http://www.nspcc.org.uk) or ChildLine Tel: 0800 1111 [www.childline.org.uk](http://www.childline.org.uk)

**Any breach of the above Information Security Policy could result in disciplinary action.**