Egerton Nursery & out of School Club

Online safety & Mobile phone Policy

Egerton Nursery and Out of School Club

EYFS: 2.1 , 3.4-3.7

Document History

Author	Kerry Hurst
Role	Manager
Approved by	Board of Directors
Approval date	18/01/2022
Review period	1 year
Review date	18/01/2023

Version History

Version	Date	Changes
4	**08.09.2022**	**Highlighted -Smart watches**
2	30/11/2020	Major overhaul to policy document.
3	11/01/2022	Changes made Added 'We refer to 'Safeguarding children and protecting professionals in early years settings: online safety considerations' to support this policy'. Updated policy throughout to reflect this document further and ensure consistency. Added section on cyber security.

List of Abbreviations Used

SENCo	Special Educational Needs Coordinator
OOSC	Out of School Club
DSL	Designated Safeguarding Lead
IWF	Internet Watch Foundation

Online Safety Policy

Our setting is aware of the growth of internet and the advantages this can bring. However, it is also aware of the dangers it can pose, and we strive to support children, staff and families to use the internet safely.

Keeping Children Safe in Education categorises online safety into three areas of risk:

- ✓ *Content: being exposed to illegal, inappropriate or harmful material*
- ✓ *Contact: being subjected to harmful online interaction with other users; and*
- ✓ *Conduct: personal online behaviour that increases the likelihood of, or causes, harm."*

The Designated Safeguarding Lead (**DSL)** is ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to **Kerry Hurst.**

Within the setting we aim to keep children, staff and parents safe online. Our safety measures include:

- Ensuring we have appropriate antivirus and anti-spyware software on all devices and update them regularly
- Ensuring content blockers and filters are on all our devices, e.g. computers, laptops, tablets and any mobile devices
- Ensuring all devices are password protected and screen locks. Practitioners are reminded to use complex strong passwords and they are kept safe and secure, changed regularly and are not written down
- Monitoring all internet usage across the setting
- Providing secure storage of all nursery devices at the end of each day
- Ensuring no social media or messaging apps are installed on nursery devices
- Reviewing all apps or games downloaded onto devices ensuring they are age and content appropriate
- Using only nursery devices to record/photograph children in the setting
- Never emailing personal or financial information
- Reporting emails with inappropriate content to the internet watch foundation (IWF www.iwf.org.uk)
- Teaching children how to stay safe online and report any concerns they have
- Ensuring children are supervised when using internet connected devices
- Using tracking software to monitor suitability of internet usage (for older children)
- Not permitting staff or visitors to access to the nursery Wi-Fi
- Talking to children about 'stranger danger' and deciding who is a stranger and who is not; comparing people in real life situations to online 'friends'
- When using Skype and FaceTime (where applicable) discussing with the children what they would do if someone they did not know tried to contact them
- Providing training for staff, at least annually, in online safety and understanding how to keep children safe online. We encourage staff and families to complete an online safety briefing, which can be found at https://moodle.ndna.org.uk

- Staff model safe practice when using technology with children and ensuring all staff abide by an acceptable use policy; instructing staff to use the work IT equipment for matters relating to the children and their education and care. No personal use will be tolerated (see acceptable IT use policy)
- Monitoring children's screen time to ensure they remain safe online and have access to material that promotes their development. We ensure that their screen time is within an acceptable level and is integrated within their programme of learning
- Making sure physical safety of users is considered including the posture of staff and children when using devices
- Being aware of the need to manage our digital reputation, including the appropriateness of information and content that we post online, both professionally and personally. This is continually monitored by the setting's management
- Ensuring all electronic communications between staff and parents is professional and takes place via the official nursery communication channels, e.g. the setting's email addresses and telephone numbers. This is to protect staff, children and parents
- Signposting parents to appropriate sources of support regarding online safety at home

If any concerns arise relating to online safety, then we will follow our safeguarding/Child Protection policy and report all online safety concerns to the DSL.

The DSL will make sure that:

- All staff know how to report a problem and when to escalate a concern, including the process for external referral
- All concerns are logged, assessed and actioned in accordance with the settings' safeguarding/Child protection procedures
- Parents are supported to develop their knowledge of online safety issues concerning their children via What's app or email
- Parents are offered support to help them talk about online safety with their children using appropriate resources
- Parents are signposted to appropriate sources of support regarding online safety at home and are fully supported to understand how to report an online safety concern.
- Staff have access to information and guidance for supporting online safety, both personally and professionally
- Under no circumstances should any member of staff, either at work or in any other place, make, deliberately download, possess, or distribute material they know to be illegal, for example child sexual abuse material

Mobile Phone and Electronic Device Use

This policy refers to all electronic devices able to take pictures, record videos, send or receive calls and messages. This includes cameras, mobile telephones, tablets and any recording devices including smartwatches. More and more devices are technically, capable of connecting us to the outside world. We will adapt the policy to include all devices we deem necessary to safeguard children.

Fitbits: depending on what the device is capable of doing, e.g. ones that receive calls and messages are prohibited but ones that only have a capacity to count steps are allowed.

Mobile phones and other devices that accept calls, messages and video calling
At **Egerton Nursery and Out of School Club** we promote the safety and welfare of all children in our care. We believe our staff should be completely attentive during their hours of working to ensure all children in the nursery receive good quality care and education.

To ensure the safety and well-being of children we do not allow staff to use personal mobile phones, smartwatches and/or Fitbits during working hours. Where smart watches are worn they must be on **DO NOT DISTURB DURING WORKING OURS OR WHEN IN THE SETTING**.

We use mobile phones supplied by the nursery to provide a means of contact in certain circumstances, such as outings.

This policy should be used in conjunction with our online safety and acceptable IT use policies, to ensure children are kept safe when using the nursery devices online.

Staff must adhere to the following:

- Mobile phones/smartwatches/Fitbits are either turned off or on **Do Not Disturb** and not accessed during your working hours
- Mobile phones/smartwatches/Fitbits can only be used on a designated break and then this must be away from the children
- Mobile phones/smartwatches/Fitbits should be stored safely in the designated place at all times during the hours of your working day
- No personal device is allowed to be connected to the setting Wi-Fi at any time
- The use of nursery devices, such as tablets, must only be used for nursery purposes
- The nursery devices will not have any social media or messaging apps on them
- Any apps downloaded onto nursery devices must be done only by management. This will ensure only age and content appropriate apps are accessible to staff, or children using them
- Passwords/passcodes for nursery devices must not be shared or written down, and will be changed regularly
- During outings, staff will use mobile phones belonging to the nursery wherever possible. Photographs must not be taken of the children on any personal phones or any other personal information storage device. Only nursery owned devices will be used to take photographs or film videos

- Nursery devices will not be taken home with staff and will remain secure at the setting when not in use. If a device is needed to be taken home due to unforeseen circumstances then the person taking this device home must ensure it is securely stored and not accessed by another other individual and returned to nursery as soon as practically possible

Parents' and visitors' use of mobile phones and smartwatches
Whilst we recognise that there may be emergency situations which necessitate the use of a mobile telephone, in order to ensure the safety and welfare of children in our care and share information about the child's day. However, parents and visitors are kindly asked to put the device on silent mode & refrain from using their mobile telephones whilst in the nursery or when collecting or dropping off their children. If you are found to be using your phone inside the nursery premises, you will be asked to finish the call or take the call outside.

We do this to ensure all children are safeguarded and the time for dropping off and picking up is a quality handover opportunity where we can share details about your child.
Visitors are requested to leave their mobile phones or smart watches in the safety of the office where they will be locked away safely.

Parents are requested not to allow their child to wear or bring in devices that may take photographs or record videos or voices. This includes smart watches with these capabilities, such as Vtech. This ensures all children are safeguarded and also protects their property as it may get damaged or misplaced at the nursery.

Photographs and videos
At **Egerton Nursery and Out of School Club** we recognise that photographs and video recordings play a part in the life of the nursery. We ensure that any photographs or recordings taken of children in our nursery are only done with prior written permission from each child's parent and only share photos with parents in a secure manner. We will obtain this permission when each child is registered and update it on a regular basis to ensure that this permission is still valid.

We ask for individual permissions for photographs and video recordings for a range of purposes including: use in the child's learning journey; for display purposes; for promotion materials including our nursery website, brochure and the local press; and for security in relation to CCTV and the different social media platforms we use. We ensure that parents understand that where their child is also on another child's photograph, but not as the primary person, that may be used in another child's learning journey. Photographs and videos will not be taken in areas where intimate care routines are carried out.

If a parent is not happy about one or more of these uses, we will respect their wishes and find alternative ways of recording their child's play or learning.

Staff are not permitted to take any photographs or recordings of a child on their own information storage devices e.g. cameras, mobiles, tablets or smartwatches and may only use those provided by the nursery. The nursery manager will monitor all photographs and recordings to ensure that the parents' wishes are met, and children are safeguarded.

Photographs or videos recorded on nursery mobile devices will be transferred to the correct storage device to ensure no images are left on these mobile devices.

Parents, and children, are not permitted to use any recording device or camera (including those on mobile phones or smartwatches) on the nursery premises without the prior consent of the manager.

During special events, e.g. Christmas or leaving parties, staff may produce group photographs to distribute to parents on request. In this case we will gain individual permission for each child before the event. This will ensure all photographs taken are in line with parental choice. We ask that photos of events such as Christmas parties are not posted on any social media websites/areas without permission from parents of all the children included in the picture.

We also do routine checks to ensure that emails and text messages (where applicable) have not been sent from these devices and remind staff of the whistleblowing policy if they observe staff not following these safeguarding procedures.

Cyber Security

This policy should be read in conjunction with your Data protection and Confidentiality Policy, Acceptable IT Use Policy and GDPR Privacy statement.

Good cyber security means protecting the personal or sensitive information we hold on children and their families in line with the Data Protection Act.
We are aware that Cyber criminals will target any type of business including childcare and ensure all staff are aware of the value of the information we hold in terms of criminal activity e.g. scam emails.
All staff are reminded to follow all the procedures above including backing up sensitive data, using strong passwords and protecting devices to ensure we are cyber secure.

To prevent any attempts of a data breach (which is when information held by a business is stolen or accessed without authorisation) that could cause temporary shutdown of our setting and reputational damage with the families we engage with we inform staff not to open any suspicious messages such as official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'.

Staff are asked to report these to the manager as soon as possible and these will be reported through the NCSC Suspicious Email Reporting Service at report@phishing.gov.uk

This policy was adopted on	**Signed on behalf of the nursery**	**Date for review**
30.11.2020		*Jan 2023*