MOSSGATE DAY NURSERY

ONLINE SAFETY POLICY

Mossgate Day Nursery is aware of the growth of internet use and the advantages this can bring. However, it is also aware of the dangers and strives to support children, staff and families in using the internet safely

We refer to *'Safeguarding children and protecting professionals in early years settings: online safety considerations'* to support this policy.

The Designated Safeguarding Lead is ultimately responsible for online safety concerns. All concerns need to be raised with them as soon as possible.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm.

The breadth of issues classified within online safety is considerable, but can be categorized into three areas of risk:

- ✓ ***Content:*** *being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;*
- ✓ ***Contact:*** *being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and*
- ✓ ***Conduct:*** *personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.*

Within the nursery 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
- Not allowing children access to the internet and all computers and tablets that may be used by the children have the internet access disabled.
- 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
- Keeping passwords safe and secure, not sharing or writing these down.
- Passwords will not be reused

- Passwords will not be stored using password managers with end-to-end encryption.
- Accounts will be removed immediately when a staff member has left employment.
- Staff will receive training in recognising when emails may contain spam, phishing or other harmful content.
- Staff must report suspicious messages or links to management.
- Employees must not install any software that has not been cleared for use by a director onto our computers or systems.
- No unknown USBs or external devices will be used.
- Monitoring all internet usage across the setting
- Ensuring no social media or messaging apps are installed on nursery devices – these sites are blocked by our internet provider
- Management reviewing all apps or games downloaded to tablets to ensure all are age appropriate for children and safeguard the children and staff
- Using approved devices to record/photograph in the setting
- Ensuring that staff do not to use personal electronic devices with imaging and sharing capabilities, including mobile phones, smart watches and cameras
- Never emailing personal or financial information except through secure email
- Reporting emails with inappropriate content to the internet watch foundation (IWF www.iwf.org.uk)
- Ensuring children are supervised when using internet devices
- Not permitting visitors 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'
- 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 is tolerated.
- 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 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 nursery's safeguarding procedures
- 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.

Cyber Security

This policy should be read in conjunction with our Data protection and Confidentiality 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 National Cyber Security Centre (NCSC) Suspicious email reporting service at report@phishing.gov.uk