Online Safety Children's Services Policy

Policy Owner: Director of Communities/SLT	**Policy Developer: Head of Family & Children's Services/AA**
Category: Policies	Version Number: [1.0]
Status: Approved	Issue Date: 17/02/2023
Date Approved: 10/02/2023	Review Schedule: Annual
Approval Level: 2	Ratified by: Q&C 17/02/2023

The current version of any policy, procedure or guideline is the version held in the Knowledge Library on Workplace. It is the responsibility of all staff to ensure that they are following the current version.

Online Safety Children's Services Policy

EYFS: 3.1-3.8

As an association are aware of the growth of internet use and the advantages this can bring. However, we are also aware of the dangers and strive 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 for each site is ultimately responsible for online safety concerns. All concerns need to be raised 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.

Keeping Children Safe in Education states *"The breadth of issues classified within online safety is considerable, but can be categorised 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 our settings we aim to keep children (and staff) safe online by:

- 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 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
- Ensure management monitor all internet activities in the setting
- Locking away all setting devices at the end of the day
- Ensuring no social media or messaging apps are installed on setting devices

- 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
- Never emailing personal or financial information
- 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 staff or visitors access to each settings Wi-Fi
- Integrating online safety into daily practice by discussing computer usage 'rules' deciding together what is safe and what is not safe to do online
- 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
- Provide training for staff that needs this 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
- We abide by an acceptable use policy; ensuring staff only use the work IT equipment for matters relating to the children and their education and care. No personal use will be tolerated
- 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
- Children's screen time is monitored to ensure they remain safe online and have access to material that promotes their development. We will 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
- Each setting is 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.
- Signposting parents to appropriate sources of support regarding online safety at home

All electronic communications between staff and parents should be professional and take place via the official communication channels, e.g. the setting's email addresses and telephone numbers and the connect childcare management system. This is to protect staff, children and parents.

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

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
- Parents are supported to develop their knowledge of online safety issues concerning their children via newsletters, emails, websites, social media and noticeboards
- 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.

Cyber Security
This policy should be read in conjunction with our 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 by	YMCA Thames Gateway Group
On	*10/02/2023*
Signed on behalf of the provider	
Name of signatory	Amanda Allen

Role of signatory (e.g. chair, director or owner)	Head of Family and Children's Services

Policy review date	10/02/2024– on or before
Name of reviewer	
Signature of reviewer	
Role of reviewer	