1.4 Online Safety

EYFS: The Safeguarding and Welfare Requirements
3.1 – 3.8

Policy Statement

Staff at Sunrise Community Nurseries (Sunrise are aware of the growth of the internet and the advantages this can bring. However, we are also aware of the dangers it can pose, and we strive to support children, staff and families to use the internet safely.

The Designated Safeguarding Lead (DSL) **Roseline Alexander** is ultimately responsible for online safety concerns. All concerns need to be raised to Roseline as soon as possible, or in her absence, the Deputy Designated Safeguarding Lead (DDSL) **Mikki Parkes**

The use of technology has become a significant component of many safeguarding issues including child sexual exploitation, radicalisation and sexual predation. Technology often provides the platform that facilitates harm.

Keeping Children Safe in Education categorises online safety 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.

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

Procedures

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
- Ensure content blockers and filters are on all our devices, for example, computers, laptops, tablets and any mobile devices
- Ensuring all devices are password protected and have timed screen locks. Passwords should be kept safe and secure, changed regularly and are not written down
- Monitoring all internet usage across the setting
- 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

- 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 to their parents or a member of the staff team.
- Ensuring children are supervised when using internet connected devices
- Not permitting 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'
- Providing training for staff, in online safety and understanding how to keep children safe online.
- Sharing, both with staff and parents, useful links to protecting children online such as
  www.nspcc.org.uk/keeping-children-safe/online-safety
  www.chilnet.com/resources/smartie-the-penguin
- Staff model safe practise when using technology with children.
- 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. (Please refer to policy **11.8 Staff Use of ICT and Social Media** for more further details).
- 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.
- We make sure physical safety of users is considered including the posture of staff and children when using devices.
- The nursery 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.
- All electronic communications between staff and parents should be professional and take place via the official nursery communication channels, e.g. email addresses and telephone numbers. 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.

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 offered support to help them talk about online safety with their children using appropriate resources.
- 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

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

Reviewed: **Currently Under Review**	Next review date: October 2023
Signed on behalf of the nursery: Mikki Parkes	