Online Safety Policy

Statement of Intent

At Bright Sparks Nursery we aware of the advantages the internet 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.

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 as soon as possible to **Alice Haigh** or in her absence one of the other DSL's **Rebecca Malone**, **Ruth Brooks**, **Amanda Walsh** or **Jade Dutton**.

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 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 the nursery, we aim to keep children and staff 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 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 unless reasonably required in the normal course of the management of the business.
- Reporting emails with inappropriate content
- 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 private access to the nursery Wi-Fi
- Talking to children sensitively and age appropriately 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 Staff Use of Mobile Phones, cameras, recording devices and smart watches 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 settings' email addresses and telephone numbers, connect childcare management system and iConnect. This is to protect staff, children and parents
- Signposting parents to appropriate sources of support regarding online safety at home usually through a newsletter from the Head of Early Years

Filtering and Monitoring

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. All software and apps are monitored by the IT Network Manager.
· The nursery maintains oversight of the Online Safety Policy contained within our main child protection policies, and the arrangements put in place to ensure appropriate filtering and monitoring on nursery devices and nursery & school networks. The appropriateness of any filtering and monitoring systems will in part be informed by the risk assessment required by the Prevent Duty as required by KCSiE 2024 paragraph138 to147. This will include:
- Identify - identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet the nursery/ school/ college safeguarding need.
- review and discuss the standards with the leadership team, IT staff and service providers to ensure the school/college meets the standard published by the Department for Education filtering and monitoring standards. Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
- At any time and without prior notice, the College maintains the right and ability to examine any systems and inspect, review and if needs be intercept any and all data recorded in those systems. Any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner may be subject to scrutiny by the College. This examination helps to ensure compliance with internal policies, supports the performance of internal investigations, and assists the management of information systems.

· A review is arranged to ensure the standards and discuss with IT staff and service providers these standards and whether more needs to be done to support our nursery/school/college in meeting and maintaining this standard and communicating these to staff, our pupils/students, parents, carers and visitors to the school who provide teaching to children as part of the learning and educational opportunities we provide.
· Ensure that all staff undergo safeguarding and child protection training, including online safety training providing an understanding of the expectations and applicable roles and responsibilities in relation to filtering and monitoring

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 supported to develop their knowledge of online safety issues concerning their children via bulletins from the Head of Early Years,

notifications from Sefton SSCP, NSPCC, NDNA or any other reputable organisations
- 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 your Data protection 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 Network Manager and Head of Early Years/ Deputy Managers as soon as possible.

New Policy November 2022
Audited Weightmans LLP 10.01.2023
Reviewed by AH – 27.09.2023
Reviewed by AH – 04.01.2024
Reviewed by AH- 30.09.2024