QUEENS PARK MONTESSORI DAY NURSERY
155 Richmond Park Road
Bournemouth
Dorset
BH8 8UA

Telephone: (01202) 523293

Proprietor: Mrs Alison Toms

Ofsted Reg: EY242933

A Unique Child
1.3 Keeping Safe

STAY SAFE

EYFS: 3.1 – 3.8

ONLINE AND E-SAFETY POLICY

At Queens Park Montessori Day Nursery we 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 and other technology safety.

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

This policy describes the rights and responsibilities of staff, children and parents using resources, such as computers, tablets, the internet, landline and mobile telephones, and other electrical equipment. It explains the procedures you are expected to follow and makes clear what is considered acceptable behaviour when using them. These devises are a vital part of our business and should be used in accordance with our policies in order to protect children, staff, and families, complying with all relevant legislations:

- Data Protection Act 2018
- General Data Protection Regulation 2018 (Regulation (EU) 2016/679)

Our appointed Online and E-Safety co-ordinator is: **Ali Pearcy (Deputy Designated Safeguarding Lead)**

The designated Safeguarding Lead (Alison Toms) is ultimately responsible for online safety concerns.

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.*

The DSL and DDSL 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
- 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. Such use constitutes misconduct and the police, LADO (Local Authority Designated Officer), and Social Care will be informed immediately. This will lead to disciplinary action up to and including summary dismissal in serious cases.

All practitioners are informed of the risks posed by adults and children who use technology, including the internet, to bully, groom, radicalise or abuse children. They oversee the safe use of technology and will take immediate action to address any concerns they encounter or that worry them.

Security and passwords

All electronic devices will be password protected by a strong password and updated as necessary, for example because of a data breach. Passwords for our systems are confidential and must be kept as such. Practitioners must not allow any other staff member to know or use their password.

Personal use of the internet, email and telephones

Any use of our electronic communication systems (including email, internet and telephones) for purposes other than the duties of your employment is not permitted.

Emergency personal calls need to be authorised by the manager and where possible, be made on your own personal mobile phone outside the nursery.

Disciplinary action will be taken where:

- the privilege of using our equipment is abused; or
- unauthorised time is spent on personal communications during working hours.

Data protection

When using any of our systems employees must adhere to the requirements of the General Data Protection Regulation 2018 (GDPR). For more information see our Data Protection and Confidentiality Policy.

Computer/laptop/tablet

- All ICT equipment will remain in the setting at all times. This is to minimise the risk of computer viruses and for data protection purposes.
- We will ensure that all programmes used, and websites accessed, are appropriate.
- We ensure we have appropriate antivirus and anti-spyware software on all laptops and they are updated regularly
- Content blockers and filters are on all our laptops and any mobile devices connected to the internet

The internet - children

Whilst the internet is now regarded as an essential part of everyday life and can be used effectively to support children's learning and development, we do not allow our children any access to the internet. As part of an adult led activity, children may watch educational videos on, for example, YouTube. They will never have unsupervised access. We do, however, teach children how to stay safe online and they are encouraged to talk to a familiar adult if they have any concerns. They are taught about 'stranger danger', who is a stranger and who is not.

Nursery ICT equipment - staff

The internet is used in the nursery to support the professional work of staff, to allow effective planning and to source resources.

- Practitioners must not use the nursery's ICT equipment for personal use (including e-mail, internet and telephones), and must not forward any information regarding children in the nursery to their home PC, laptop, tablet, phone, etc. Emergency personal calls must be authorised by the manager.
- Before using any removable storage media which has been used on hardware not owned by the nursery (for example, USB pen drive, CDROM, etc.) the contents of the storage device must be virus checked. Removable devices must not be taken home unless under exceptional circumstances and authorised to do so by the management team, with prior written permission and risk assessment in place.
- Practitioners must not access, copy, remove or otherwise alter any other user's files without their permission.
- Practitioners must not install or store programmes of any type or try to alter any computer/laptop/tablet settings, unless permission has been granted and changes are in line with current legislation, guidance, policies and procedures.
- Practitioners must abide by all security measures, including creating and using strong passwords.

Each employee has a responsibility to report any misuse of the internet or e-mail. By not reporting such knowledge, the employee will be considered to be collaborating in the misuse. Each employee can be assured of confidentiality when reporting misuse. The equipment must not be used, removed, or destroyed.

All staff are to complete an online e-safety briefing during the enrolment process, and annually after this. This can be found at www.moodle.ndna.org.uk

E-mail
E-mail is a useful way of communicating with parents about their child and current activities at the nursery and we expect all staff to use their common sense and good business practice when using e-mail. As e-mail is not a totally secure system of communication and can be intercepted by third parties, external email should not normally be used in relation to confidential transactions. We will:

- Never send out any personal or financial information about the child or parent over e-mail unless the contents have been encrypted.
- Never send pictures of children via e-mail and, if parents choose to do this, we will inform them of the risks involved in this so they may make an informed choice
- Never divulge e-mail addresses to any other parent unless permission is given.
- Send all group e-mail by BCC.
- Keep all login details on a strictly need to know basis.
- Ensure all e-mails sent to parents are from the nursery/room e-mail accounts, never from a private or personal e-mail address.
- Ensure the nursery e-mail addresses are not used for personal e-mail.
- All e-mail communication is appropriate and written in a professional manner, and is not used to send abusive, offensive, sexist, racist, disability-biased, sexual orientation based or defamatory material, including jokes, pictures, or comments which are potentially offensive. Any such messages must be brought to the attention of the manager as they may constitute harassment and/or discrimination. This may lead to disciplinary action up to and including summary dismissal.
- E-mail attachments are only be opened if they are from a source known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- Report e-mails with inappropriate content to the internet watch foundation (IWF www.iwf.org.uk/)
- Ensure children have no access to e-mail.

The internet – parents

- All parents are required to read and sign the e-safety policy as part of their induction. If a parent does not wish their child to access the internet at all then they should inform their child's key-worker.
- Photographs taken by parents at nursery outings or events must be for personal use only and must not be uploaded to any social networking sites if the image contains children other than their own unless permission has been given by all parents.
- Parents must not make comments on social media about other children in the nursery without permission from the relevant parent.
- Children must not bring in their own equipment that may be enable them to access the internet, take photos, or record audio.
- Parents are supported to develop their knowledge of online safety issues concerning their children via letters and information leaflets sent home
- 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

Webcams
The webcams on each nursery laptop are covered by a sticker at all times. Webcams will not be used in the nursery.

Computer software

- All educational software used with the children is suitable and appropriate for the ages of the children in our care. Only children in the Montessori room have supervised access to computer software on their own laptop. This laptop is not connected to the internet.
- The nursery is legally compliant when purchasing software according to the number of users. All educational software are originals and not copies.
- Employees may not install any software that has not been cleared for use by the manager. Such action may lead to disciplinary action up to and including summary dismissal in serious cases.

Online Learning Journals (Learning Book)

- The system used at Queens Park Montessori Day Nursery is Learning Book. They are a fully reputable provider who guarantee the security of data put into the system.
- The tablets used for our online learning journals are dedicated for this purpose. They only contain the Learning Book software with no access to any other apps.
- Parents are fully informed about the Learning Book and how it works during their induction process. They are required to give permission for their children's pictures/videos to be used in their own journal and those of the other children. They are given an information pamphlet with all relevant information when they sign up.
- Parents are shown how to access their child's information. They must input their e-mail address and will then be able to set their own strong password. They are informed about the importance of keeping the password safe and not sharing with anyone they do not wish to access their child's information. The nursery has no access to the passwords.
- All practitioners are given a full explanation of how the Learning Book works once they have received their enhanced DBS certificate. They are not allowed access to the online facility until this has been received.

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. This is continually monitored by the management.

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

This policy was adopted on*:* ……

Signed on behalf of the nursery: ……..

Date for review: ……