Online Safety Policy and Procedure

Including Staff Acceptable Use Policy

Townsend Montessori Nurseries Limited believe that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets and mobile phones.

The purpose of Townsend Montessori Nurseries Limited online safety policy is to:

- Clearly identify the key principles expected of all members of staff with regards to the safe and responsible use of technology to ensure that the nursery is a safe and secure environment.
- Safeguard and protect all members of staff online.
- Raise awareness with all members of staff regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all access to the internet and use of information communication devices i.e tablets in rooms to record children's development.

This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, behaviour, data protections and confidentiality.

Key responsibilities of the setting management team are:

- Developing, owning and promoting the online safety vision and culture to all staff
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the setting
- Keeping passwords safe and secure, not sharing or writing these down
- Not permitting staff or visitors access to the nursery Wi-Fi

- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.

- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.

Key responsibilities of the designated safeguarding/online safety lead are:

The Designated Safeguarding Lead is: _____

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends.
- Ensuring that online safety is promoted to parents and carers through a variety of channels and approaches.
- Ensure practice is in line with legislation regarding data protection.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the settings safeguarding recording structures and mechanisms.
- Liaising with the local authority and other local and national bodies as appropriate.
- Ensuring that online safety is integrated with other appropriate policies and procedures.

Key responsibilities of staff are:

- Contributing to the development of online safety policies.
- Reading the settings policies and adhering to them.
- Taking responsibility for the security of setting systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies
- Integrating online safety into nursery 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'

- 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.
- Staff will ensure that all images are used in accordance with the setting image use policy.
- Use of the webcam is not permitted

- Identifying individuals of concern and taking appropriate action by working with the designated safeguarding lead.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.

- Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the safeguarding lead.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.

Key responsibilities of parents and carers are:

- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Seeking help and support from the setting, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the settings online safety policies.
- Using setting systems safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Managing email:

- The use of personal email addresses by staff for any official setting business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Staff must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school online safety incident
- Information shared via email will be in accordance with data protection legislation.
- Access to external personal email and social media sites is not permitted
- The setting will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the settings leadership team.

Engagement and education of staff:

The online safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of the settings safeguarding practices.

Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.

Managing personal data online:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998, and General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR)

Security and Management of Information Systems:

- The security of the school information systems and users will be reviewed regularly.

- Virus protection will be updated regularly.
- Portable devices i.e tablets are not to be remove from the setting
- Unapproved software will not be authorised
- Files held on the school's network will be regularly checked.
- All users will be expected to log off or lock their screens/devices if systems are unattended.

Management of applications (apps) used to record children's progress

- The Nursery Manager is ultimately responsible for the security of any data or images held of children.
- Systems which store personal data will be risk assessed prior to use.
- Personal devices will not be used for any apps which record and store children's personal details, attainment or photographs.

Please also refer to the Mobile Phone Policy for information regarding use of cameras

Staff Acceptable Use Policy

To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the nursery's systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the company ethos, other appropriate policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. Nursery information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the Area Manager / Operations Manager.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998 and General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR)This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place. Any images or videos of children will only be used as stated in the nursery policy and will always take into account parental consent.

7. I will not keep or access professional documents which contain nursery-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones). I will protect the devices in my care from unapproved access or theft.

8. I will not store any personal information on the nursery computer system including any nursery laptop or similar device issued to members of staff that is unrelated to nursery activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (name) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (name) Designated Safeguarding Lead.

11. My electronic communications with parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via nursery approved communication channels e.g. via a nursery provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones.

12. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using nursery or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

13. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the nursery into disrepute.

14. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

15. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead (name)

16. I understand that my use of the nursery information systems (including any devices provided by the nursery) and nursery email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

The company may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the nursery's information system or unacceptable or inappropriate behaviour may be taking place, the company will invoke its disciplinary procedure. If the company suspects that the nursery system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

This policy was adopted on	**Date for Review**
19.12.19	*December 2020*