New Millside Pre-school

TECHNOLOGY USAGE POLICY

Purpose

This policy sets out the rules for using shared computers, the preschool mobile phone, staff-issued tablets, and associated email accounts to ensure security, data protection, and responsible use.

Scope

This policy applies to all staff members who use any device or email account provided by New Millside Pre-School, including shared computers, the preschool mobile, individual tablets, and work-related email addresses.

General Rules (Apply to All Devices & Accounts)

- All communication must be professional and in line with safeguarding and confidentiality policies.
- Do not open suspicious emails, attachments, or links. Report anything unusual immediately.
- Failure to comply with this policy may result in disciplinary action.

Policy Guidelines

1. General Equipment Use

- All equipment is for work-related tasks only.
- Only authorised apps may be downloaded/used (e.g., Tapestry).
- Photos/Videos must be removed from storage as soon as they are uploaded to the child's online learning journal or are no longer required.
- Under no circumstances will photos/videos be backed up online.
- Handle all personal information about children in accordance with data protection legislation. Personal information must not be shared with unauthorised persons.
- Care must be taken with equipment (charging ports, screen cleaning, cases/bags provided, antivirus checks, password updates, etc.).
- Notify the Administration & Finance Manager immediately if equipment is lost, stolen, infected with a virus, not working properly, or if passwords are updated. Do not attempt repairs or allow unauthorised personnel to do so.
- Safeguarding and Managers will carry out equipment 'spot checks'.
- Equipment must not be taken home unless under exceptional circumstances and signed out with management. It must be returned the next day.
- If equipment is damaged (excluding normal wear and tear or accidental damage), lost, or stolen outside company premises because it was not kept in a secure location, the staff member will be responsible for the cost of repair or replacement.
- Upon leaving the company, all equipment must be returned in good working order. Failure to do so may result in payroll deductions for replacement costs.

2. Shared Computer Usage

- Shared computers are for work-related tasks only (e.g., printing resources, accessing Tapestry or approved training platforms such as Flick, Bucks CPD).
- The assigned email account (e.g., sharedpc@newmillsidepre-school.co.uk) is for internal use only and must not be used to email parents or external parties.
- If you sign into your individual training/Tapestry accounts, you must sign out before leaving the computer.
- Do not save passwords or enable auto-login features.
- Only access permitted websites approved by management. Personal browsing, social media, or streaming sites are strictly prohibited.
- Do not download or store personal data on the shared computer.
- If staff need to save documents, they should save them in the 'Documents' folder and create a new sub-folder with their staff name. Be aware that these folders can be accessed by all staff, so do not save anything that is confidential or not intended for everyone to see. If resources are general/for everyone (e.g., Twinkl), they should be saved in the 'Resources' folder.
- Staff must record their name, date, time in, and time out in the shared computer logbook each time they use the computer. This log will be kept next to the computer and checked by management for monitoring and safeguarding purposes.
- Do not install unauthorised software or apps.
- Run regular Norton antivirus scans as instructed by management.
- Management reserves the right to carry out spot checks to ensure compliance.

3. Preschool Mobile Phone Usage

- The preschool mobile is the official communication channel with parents.
- It must only be used for work-related communication, including parent updates, emergency contact, and authorised calls/messages/updating WhatsApp Community.
- Do not use the mobile for personal calls, texts, or social media.
- Photos/videos taken on the mobile must be deleted from the device.
- Do not back up photos/videos to any online storage or personal accounts.
- Keep the mobile secure at all times and report any loss or damage immediately.
- Do not install unauthorised apps or change settings without permission.

4. Staff Tablets & Email Accounts

- Staff who are issued individual tablets must comply with the same rules outlined above for equipment use.
- A record will be kept of all equipment assigned to staff.
- Tablets are not issues until this policy and our Tapestry Policy has been read and signed to confirm they understand their responsibilities.
- Staff may be provided with a work domain email or a Gmail account for tablet setup (e.g., for Tapestry access).
- Gmail accounts and the sharedpc email are not to be shared externally and no parents are to be contacted from these accounts.
- These email accounts are strictly for work purposes only.
- Personal email accounts must not be accessed on work tablets.
- Regular antivirus scans must be run on tablets.

5. Artificial Intelligence (AI) Usage

- AI tools may only be used for work-related tasks and must be approved by management.
- Do not input personal information about children, parents, or staff into AI tools (including names, addresses, photos, or sensitive data).
- AI-generated content must be reviewed and verified by staff before use. Do not rely solely on AI for factual accuracy.
- AI tools must never be used to communicate directly with parents or children.
- Only use AI tools on approved devices and platforms. Do not use personal accounts or unverified AI services.
- If AI-generated content is used in official documents or communications, it should be disclosed where appropriate.
- Management reserves the right to review AI usage and ensure compliance.

Monitoring & Enforcement

Management will monitor compliance through spot checks and system audits. Breaches of this policy may lead to disciplinary action.

This policy should be read alongside the e-Safety Policy for guidance on safeguarding and online safety for children.