



Secure Handling Policy

Updated September 2024

The purpose of this policy is to ensure that all sensitive information, materials, and resources within the nursery are handled securely to protect the privacy, safety, and integrity of children, families, staff, and the nursery itself. This policy establishes clear guidelines for the secure handling of physical and digital information, resources, and equipment. This policy applies to all nursery staff, volunteers, management, and any third parties who handle sensitive or confidential materials related to the nursery.

Secure Handling of Personal and Confidential Information:

Confidentiality and Privacy:

- All personal information related to children, parents, and staff (e.g., medical records, contact information, attendance records) must be treated as confidential and must not be shared without consent unless required by law or child protection protocols.
- Access to confidential information should be restricted to those staff members who require it for their work responsibilities.

Data Storage:

- **Physical Information:** Paper-based documents containing confidential information must be stored securely in locked filing cabinets or secure areas.
- **Digital Information:** Digital records containing sensitive data must be stored on password-protected computers or secure systems with encryption.
- **Data Back-Up:** A secure backup system for digital records should be in place to ensure information is not lost due to system failure.

Access Control:

- Only authorised personnel should have access to sensitive or confidential information. Access should be granted based on the principle of “need to know” for staff roles.
- Staff must ensure they log out or lock devices when leaving them unattended to prevent unauthorised access to confidential data.

Disposal of Confidential Information:

- **Physical documents:** Any confidential paper records must be shredded before disposal to prevent unauthorised access.
- **Digital information:** Digital records or files that are no longer required should be securely deleted from all devices, including cloud storage or backup systems.

Secure Handling of Children's Belongings and Medications:

Children's Belongings:

- Children's personal belongings (e.g., clothes, toys, and other items) should be stored safely in designated areas to prevent loss or mix-ups. These areas should be secure and monitored regularly.

Medications and Health Records:

- Medications must be securely stored in locked cabinets, and only authorised staff members should have access to them. Specific medication guidelines and permission slips from parents must be adhered to.
- Health records, including allergy or medical condition information, must be handled in a confidential manner and only shared with staff who need the information to ensure the safety and well-being of the child.

Emergency Information:

- Emergency contact information and any important medical details about children (e.g., allergies, conditions, or specific needs) should be stored securely but be readily accessible to staff in case of an emergency.

Secure Handling of Financial Information:

Payment and Billing Information:

- All financial records, such as billing information for parents/guardians and payments made, must be securely handled.
- Payment details (e.g., bank account numbers, credit card information) should not be written down or stored in an unsecured manner. Financial records must be stored digitally in encrypted systems or securely locked physical areas.

Fundraising and Donations:

- Any funds raised or donations collected for the nursery should be handled and accounted for securely, with proper documentation to prevent misuse.

Secure Handling of Nursery Resources and Equipment:

Key Control:

- Keys to the nursery's premises must be stored securely when not in use. A key register should be maintained, recording who has access to the keys and when they are used. The number of staff members with keys should be kept to a minimum to ensure security.

Equipment and Resources:

- Nursery equipment, especially items that are expensive, sensitive, or hazardous (e.g., cleaning supplies, technology, or electrical equipment), should be stored in secure areas when not in use to prevent loss or unauthorised access.

Technology and Devices:

- Laptops, tablets, and other electronic devices should be stored securely when not in use. Devices must be password-protected and, where possible, encrypted.
- Any device that contains sensitive information should be kept in a locked area when not in use and never left unattended in public or unsupervised spaces.

Training and Awareness:

Staff Training:

- All staff members will be trained on the importance of secure handling of confidential information, resources, and equipment. This training will cover topics such as data privacy, key control, safe storage, and handling of sensitive materials.

Ongoing Awareness:

- The nursery will regularly reinforce the importance of secure handling through meetings, updates, and reminders. Any staff members who fail to comply with this policy will be subject to appropriate corrective action.

Incident Reporting and Response:

Reporting Breaches:

- Any breach of security, such as a lost key, unauthorised access to confidential information, or any other incident, must be reported to the management immediately.
- The nursery will investigate the breach and take corrective measures to prevent similar incidents from occurring in the future.

Corrective Action:

- If a staff member or third party is found to have mishandled confidential information or resources, appropriate corrective actions will be taken. This may include retraining, disciplinary action, or, in extreme cases, termination.

By adhering to this Secure Handling Policy, the nursery will ensure that all sensitive information, materials, and resources are handled with the highest level of care and confidentiality. This policy is intended to protect the privacy and security of children, staff, and families, while maintaining the integrity and safety of the nursery environment.

Review of Policy:

This policy will be reviewed annually (September 2025), or as needed, to ensure that it remains relevant and effective in meeting the evolving needs of the children, families, and staff within the nursery.

Name:	Position:	Signed:	Date:
David Birkbeck	Owner		
Kayleigh Tydd	Director		
Greg Bamber	Nominated Individual		
Zoe Tydd	Manager & DSL		
Abbie Lloyd	Deputy Manager		
Jade Radcliffe	Second Deputy Manager		
Pamela Lear	Practitioner		
Diane Jones	Practitioner		
Emily Gautrey	Practitioner		