Confidentiality and Client Access Policy

Policy Statement

Our setting is committed to maintaining the highest standards of confidentiality. We recognise our duty to protect the privacy of children, families, and staff by handling all personal information in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Early Years Foundation Stage (EYFS) statutory framework.

All information shared with the setting is treated respectfully, stored securely, and used only for legitimate purposes.

Aims

- To protect the personal information of children, families, and staff.
- To ensure information is shared appropriately, safely, and lawfully.
- To provide parents/carers with clear guidance on how they can access personal information held about their child.
- To ensure staff understand their responsibilities regarding confidentiality.

Types of Information Held

We may hold the following:

- Child registration information
- Emergency contacts
- Medical information and dietary needs
- Attendance and safeguarding records
- Accident and incident forms
- Assessments, observations, and learning records

- Staff employment information
- Financial and invoicing records

All information is held only as long as necessary and in accordance with legal retention requirements.

Confidentiality Principles

Sharing of Information

- Information will only be shared with staff on a need-to-know basis to ensure safe and effective care.
- Information may be shared with external professionals (e.g., health visitors, SENCO, social workers) only with parental consent, unless required by law.

When Information May Be Shared Without Consent

Information may be shared without consent when:

- A child is at risk of harm or abuse.
- A crime may have been committed.
- Disclosure is required by law or court order.
  In these instances, the Designated Safeguarding Lead (DSL) will decide in line with safeguarding legislation and local authority guidance.

Storage and Security of Information

- Paper records are stored in locked cabinets.
- Digital data is stored on password-protected systems with restricted access.
- Staff are prohibited from storing personal data on personal devices unless authorised.
- Emails containing personal information are sent securely.

Staff Responsibilities

All staff, students, and volunteers must:

- Maintain confidentiality at all times.
- Not discuss children, families, or staff outside the setting.
- Not post any information relating to the setting on social media.
- Report any data breaches immediately to the Manager/Designated Person.

Any breach of confidentiality will be treated as a disciplinary matter.

Parents' and Carers' Access to Information

Parents/carers have the right to:

- Access personal information held about their child under UK GDPR (Subject Access Request).
- Request correction of inaccurate information.
- Request how and why data is used.

Procedures for Access

- Requests must be made in writing.
- The setting will respond within one month of the request.
- Identification may be required before information can be shared.
- Information relating to other children or individuals will not be disclosed.

Access to Learning and Development Records

Parents may view:

- Learning journals/portfolios
- Progress reports
- Observations

These can be discussed during parent meetings or by arrangement with the child's key person.

Information We Cannot Share

We cannot share:

- Information that identifies another child or family.
- Child protection or safeguarding records, unless authorised by statutory agencies.
- Staff personal data (other than information parents are legally entitled to).

Client Confidentiality in Daily Practice

- Conversations about children will take place in private areas.
- Visitors and contractors will not have access to personal data.
- Registers, files, and screens are kept out of public view.
- Photographs or videos are taken only with parental consent and used according to our Photography and Social Media policies.

Data Retention

Records will be kept for the required legal period, such as:

- Accident records – until the child is 21 years and 3 months
- Child records – usually 3–6 years after leaving
- Safeguarding records – until the child is 25

A full retention schedule is available on request.

Data Breaches

Any data breach will be:

- Investigated immediately
- Recorded in the data breach log
- Reported to the ICO (Information Commissioner's Office) within 72 hours if there is a risk to individuals

Affected families will be informed as required.

This policy was adopted in March 2024.

It will be reviewed annually or as required.

Last updated: 07.07.26

Signed by Chair of Trustees: 

Signed by Operations Manager: