Mapledene Children's Centre

Data Retention Policy

Purpose

This policy outlines how Mapledene Children's Centre manages, stores, and retains personal data in accordance with applicable data protection laws, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It ensures that information is kept only for as long as necessary and disposed of securely.

Scope

This policy applies to all staff, volunteers, contractors, and third parties who handle personal data on behalf of the Centre. It covers all formats of data, including paper records, digital files, emails, photographs, and recordings.

Principles

Mapledene Children's Centre follows these key principles:

Personal data will not be kept longer than necessary.

Retention periods will be based on legal, regulatory, and operational requirements.

Data will be reviewed regularly to ensure it remains accurate and relevant.

Data that is no longer required will be securely deleted or destroyed.

Categories of Data and Retention Periods

Child Records (including registration, assessments, safeguarding information):

Retained until the child reaches 25 years of age (or longer if safeguarding concerns require).

Safeguarding and Child Protection Records:

Retained in line with local authority guidance, typically until the child reaches 25 years old.

Attendance Records:

Retained for 3 years after the last date of attendance.

Staff Records (including recruitment, employment, training):

Retained for 6 years after employment ends.

Accident and Incident Reports:

Retained for a minimum of 3 years; for children, retained until age 21.

Financial Records (invoices, payroll, accounts):

Retained for 6 years in accordance with HMRC requirements.

Consent Forms (e.g., photos, data sharing):

Retained while valid and for up to 3 years after expiry.

Email Correspondence:

Retained for a maximum of 3 years unless required for legal or safeguarding purposes.

CCTV Footage (if applicable):

Retained for 30 days unless required for investigation.

Storage and Security

Paper records will be stored in locked cabinets with restricted access.

Electronic records will be stored on secure, password-protected systems.

Access to personal data will be limited to authorised personnel only.

Regular backups and security measures will be in place to prevent data loss or breaches.

Disposal of Data

Paper records will be shredded or disposed of using confidential waste services.

Digital data will be permanently deleted using secure methods.

Devices containing personal data will be wiped before disposal or reuse.

Responsibilities

The Centre Manager is responsible for ensuring compliance with this policy.

All staff are responsible for adhering to retention guidelines and reporting any concerns.

Data protection responsibilities will be included in staff training and induction.

Review and Monitoring

This policy will be reviewed annually or sooner if there are changes in legislation or operational requirements. Regular audits will be conducted to ensure compliance.

Breach and Non-Compliance

Failure to comply with this policy may result in disciplinary action. Any data breaches must be reported immediately in line with the Centre's Data Protection and Breach Policy.

Contact

For questions about this policy or data protection practices, please contact the Centre Manager or designated Data Protection Lead.

Approved by: _____

Date: _____

Review Date: _____