DATA PROTECTION AND CONFIDENTIALITY POLICY

1. Statement of Intent

At everyFAMILY Nursery we recognise our responsibility to handle personal data lawfully, fairly and transparently. We collect and process personal data relating to children, parents/carers, staff and visitors in order to provide safe, high-quality childcare and to meet our legal obligations.

We are committed to complying with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Early Years Foundation Stage (EYFS) Statutory Framework (2024)

---

2. Scope

This policy applies to:

- All staff, students and volunteers
- All personal data held in paper or electronic form
- All information relating to children, families, staff and third parties

---

3. Roles and Responsibilities

Data Protection Lead:
Michelle McQuarrie – HR & Business Operations Manager

The Data Protection Lead is responsible for:

- Overseeing GDPR compliance
- Managing data breaches
- Responding to subject access requests

All staff are responsible for protecting personal data and following this policy.

---

4. Lawful Basis for Processing

We process personal data under the following lawful bases:

Purpose	Lawful Basis	Special Category Condition
Delivering childcare services	Contract	N/A
Meeting EYFS/legal obligations	Legal obligation	Substantial public interest
Safeguarding children	Public task	Vital interests / safeguarding
Maintaining records & planning	Legitimate interests	N/A
Health, dietary & medical needs	Legal obligation	Health or social care

---

5. Systems We Use

We use secure systems to process and store data, including:

- **Famly** (attendance, billing, communication and records)
- **CPOMS** (safeguarding and child protection records)
- **Noodle Now** (staff training and compliance)
- **BreatheHR** (staff HR and personnel records)
- **CRM via Rakatatech** (enquiries and communication records)

These systems act as **data processors** on our behalf. We remain the **data controller** responsible for the data and ensure all providers comply with UK GDPR requirements.

---

6. Data We Collect

We may collect:

- Child details (name, DOB, address)
- Parent/carer contact details
- Emergency contacts
- Medical and dietary information
- Safeguarding records
- Attendance and learning records
- Photographs and observations
- Staff employment records

---

7. Data Storage and Security

We ensure appropriate security measures including:

- Locked filing cabinets for paper records
- Password-protected systems
- Role-based access controls
- Secure cloud-based systems (Famly, CPOMS, Noodle Now, BreatheHR, CRM)
- Encryption where appropriate
- Regular data backups
- Staff training on data protection and cyber security

Personal data is only accessed on a **need-to-know basis**.

---

8. Data Sharing

We may share information where necessary with:

- Local Authority
- Ofsted
- Health professionals (GPs, Health Visitors)
- Social care services
- Emergency services

We only share data when:

- We have consent, OR
- There is a legal or safeguarding obligation

We do not use personal data for marketing purposes.

---

9. Data Retention

We retain records in line with legal and safeguarding requirements:

- Child records and Accident: until age **21 years and 3 months**
- Safeguarding records: **25 years**
- Staff records: **6 years after employment ends**

Data is securely deleted, shredded or anonymised when no longer required.

10. Data Subject Rights

Individuals have the right to:

- Access their data (Subject Access Request)
- Request correction of inaccurate data
- Request erasure (where applicable)
- Restrict processing
- Object to processing
- Data portability
- Lodge a complaint with the Information Commissioner's Office (ICO)

Requests will be responded to within **one month**.

---

11. Confidentiality

All staff, students and volunteers must:

- Keep information confidential
- Not discuss children or families outside the setting
- Only share information with authorised persons

Breaches of confidentiality may result in disciplinary action.

---

12. Safeguarding

Safeguarding overrides confidentiality. Information may be shared without consent if:

- A child is at risk of harm
- Sharing is necessary to protect a child

All safeguarding concerns are recorded securely and shared only with relevant professionals.

---

13. Data Breach Procedure

A data breach includes loss, theft, or unauthorised access to personal data.

In the event of a breach we will:

1. Report immediately to the Data Protection Lead (Michelle McQuarrie)
2. Contain and assess the breach
3. Record the incident
4. Report to the ICO within **72 hours** where required
5. Inform affected individuals where there is a high risk

---

14. Training

All staff receive:

- GDPR and confidentiality training at induction
- Regular refresher training

---

15. Monitoring and Review

This policy will be reviewed annually or sooner if legislation changes.

---

16. Related Documents

- Privacy Notice (Parents & Carers)
- Staff Privacy Notice
- Safeguarding Policy
- IT & Acceptable Use Policy
- Records Retention Schedule

Date of Policy: 19 June 2026

Review Date: 19 June 2027