

Safeguarding and Data Protection Policy

How We Handle Sensitive Information Under UK GDPR

Purpose

This policy explains how we, as an early years setting, handle sensitive safeguarding data and staff contact information in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1. Safeguarding Children's Data

We have a legal duty to keep children safe. This includes recording and, when necessary, sharing information about concerns regarding a child's safety or welfare. These records may include:

- Observations, disclosures, or concerns raised
- Actions taken and who was involved
- Communications with external safeguarding services

We **do not** require parental consent to record concerns and responses or share safeguarding information when:

- It is needed to protect a child's well-being or safety.
- It is part of our legal obligation under safeguarding legislation (e.g. Children Act 1989, KCSIE)
- It forms part of our public duty under the Early Years Foundation Stage (EYFS) framework

These records are stored securely within our online system (On the Button) and are only accessible to the Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (DDSL) or authorised senior staff.

Retention: Safeguarding records are kept in line with statutory guidance; typically, until the child's 21st birthday, where a concern or file exists.

2. Staff Contact Information

We collect and store basic personal information about staff to enable them to carry out their roles safely and effectively. This includes:

- Full name
- Mobile phone number
- Role within the setting
- Access permissions to the digital platform

This data is processed under the lawful basis of **legitimate interests** and/or **contractual necessity**. For example:

- To ensure the right people can access and record safeguarding information
- To enable staff to receive system notifications or emergency communications
- To provide login credentials for secure software access to our safeguarding recording system, "On the Button".

Staff names may appear in records such as observations, safeguarding notes, and complaints to maintain accurate and auditable logs of who took what action.

Access: Staff contact details are only visible to authorised team members and are never shared externally without consent or legal requirements.

Furthermore, we cover information recorded as part of our safer recruitment processes, training logs, and may include future features On the Button publishes. These features and records help us meet our responsibilities as an employer and support staff development and accountability.

3. Security and Your Rights

All safeguarding and staff data is:

- Stored securely with role-based access controls.
- Encrypted where applicable.
- Never shared unless legally required or with explicit permission.

You have the right to:

- Request access to your personal data (note: access to safeguarding records may be limited if releasing them could compromise a child's safety, an ongoing investigation, or the privacy of other individuals such as family members)
- Ask for corrections to inaccurate information
- Raise concerns with the setting or the Information Commissioner's Office (ICO)

Questions or Concerns?

Please speak to our GDPR Officer: Laura Furniss