

Data Protection and Confidentiality Policy

Purpose

EDG Nursery is committed to protecting the privacy, confidentiality and security of all children, families, staff, students and visitors.

The nursery collects and processes personal information to fulfil its responsibilities in providing safe, high-quality childcare and education. All information is handled in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and relevant safeguarding legislation.

This policy outlines how confidential information is managed, shared, stored and protected within the nursery.

Principles of Data Protection

EDG Nursery will ensure that all personal information is:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date
- retained only for as long as necessary
- stored securely and protected against unauthorised access
- processed in a manner that ensures appropriate security and confidentiality

Confidentiality

Children, families and staff have a right to expect that information held by the nursery will be treated respectfully and confidentially.

All staff, students, volunteers and visitors are expected to maintain confidentiality at all times.

Confidential information may include:

- personal details
- medical information
- safeguarding concerns
- assessment and development records
- SEND information
- family circumstances
- staff employment records
- payroll information
- disciplinary or grievance matters

Confidential information must only be accessed by individuals who have a legitimate professional need to know.

Staff Responsibilities

All staff are responsible for protecting confidential information.

Staff must:

- follow nursery policies and procedures
- maintain confidentiality at all times
- access information only when required for their role
- store information securely
- report concerns regarding data security immediately
- ensure conversations regarding children and families remain professional and private

Staff must not:

- discuss confidential information outside of work
- discuss children or families in public places
- access records unnecessarily
- share confidential information with unauthorised individuals

- leave confidential information unattended
- remove confidential information from the nursery without authorisation

Confidentiality obligations continue after employment or placement has ended.

Information Sharing

The nursery recognises the importance of information sharing in supporting children's welfare and development.

Information will only be shared where:

- parental consent has been obtained
- there is a legal obligation to do so
- it is necessary to protect a child or vulnerable person
- safeguarding concerns require information to be shared
- information is requested by an authorised agency acting within its legal powers

Information shared will always be:

- relevant
- proportionate
- accurate
- timely
- shared securely

Safeguarding and Confidentiality

The welfare of the child is paramount.

Staff must never promise confidentiality to a child if there are any safeguarding concerns exist.

Where a child may be at risk of harm, information may be shared without consent in accordance with safeguarding legislation and local safeguarding procedures.

All safeguarding concerns must be reported to the Designated Safeguarding Lead (DSL) or Deputy DSL immediately.

Electronic Information

The nursery uses secure electronic systems to store and manage information.

Electronic records may include:

- children's learning journeys
- attendance records
- funding information
- safeguarding records
- staff records
- training records

Electronic information must only be accessed through authorised nursery systems.

Staff must not:

- store nursery information on personal devices
- use personal email accounts for nursery business
- transfer confidential information to unauthorised devices
- save nursery documents to personal cloud storage systems
- share passwords with other individuals

Passwords must be kept secure and changed when required.

Artificial Intelligence (AI)

To protect the privacy of children, families and staff, information must not be uploaded to artificial intelligence (AI) platforms without explicit authorisation from the nursery.

This includes:

- children's names
- photographs
- observations
- assessments
- safeguarding information
- medical information
- staff records
- confidential nursery documentation

Any use of AI systems must comply with UK GDPR and nursery data protection procedures.

Photography, Video and Images

Photographs and videos of children will only be taken using authorised nursery devices and in accordance with parental permissions.

Staff must not:

- use personal mobile phones to photograph children
- store images of children on personal devices
- share photographs through personal messaging services or social media

All images must be stored securely within approved nursery systems.

Data Breaches

A data breach occurs when personal information

- lost
- stolen
- accessed without authorisation
- disclosed inappropriately
- altered without permission

Any actual or suspected data breach must be reported immediately to the Nursery Manager or Directors.

The nursery will investigate breaches promptly and take appropriate action to minimise risk and comply with legal requirements.

Training

All staff will receive information regarding:

- confidentiality
- safeguarding information sharing
- data protection responsibilities
- secure handling of information
- GDPR requirements

Training will be refreshed regularly as part of staff induction and ongoing professional development.

Monitoring and Compliance

The nursery will regularly monitor:

- information security arrangements
- storage systems
- access permissions
- record keeping practices
- confidentiality procedures

Any concerns identified will be addressed promptly.

Related Policies

This policy should be read alongside:

- GDPR Privacy Notice
- Record Retention Policy
- Access and Storage of Information Policy
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Mobile Phones and Electronic Devices Policy
- Staff Conduct and Professional Boundaries Policy