

Data Protection Policy

Context and Overview

Introduction

Grass Roots Private Day Nursery Ltd needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

Why this policy exists

This data protection policy ensures Grass Roots Private Day Nursery Ltd:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

The General Data Protection Regulations (GDPR) 2018 describe how organisations – including Grass Roots Private Day Nursery Ltd – must collect, handle and sort personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

People, risks and responsibilities

Policy Scope

This policy applies to:

- All management, staff and volunteers of Grass Roots Private Day Nursery Ltd.
- All contractors, suppliers and other people working on behalf of Grass Roots Private Day Nursery Ltd.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus any other information relating to individuals

Data protection risks

This policy helps to protect Grass Roots Private Day Nursery Ltd from some very real data security risks, including:

- Breaches of confidentiality, for instance, information being given out inappropriately.
- Failing to offer choice, for instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage, for instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Grass Roots Private Day Nursery Ltd has some responsibility for ensuring the data is collected, stored and handled appropriately.

Everyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Grass Roots Private Day Nursery Ltd meets its legal obligations.
- The Data Protection Officer, Matthew Pottinger, is responsible for:
 - Keeping the board updated about data protection responsibilities, risks and issues.
 - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
 - Arranging data protection training and advice for the people covered by this policy
 - Handling data protection questions from staff and anyone else covered by this policy.
 - Dealing with requests from individuals to see the data Grass Roots Private Day Nursery Ltd holds about them (also called 'subject access requests').
 - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
 - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
 - Performing regular checks and scans to ensure security hardware and software is functioning properly.
 - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
 - Approving any data protection statements attached to communications such as emails and letters.
 - Addressing any data protection queries from journalists or media outlets like newspapers.
 - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line manager.
- Grass Roots Private Day Nursery Ltd will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data protection officer.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives, and should only be uploaded to an approved cloud computing service.
- Data should be backed up frequently.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to Grass Roots Private Day Nursery Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure that the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires Grass Roots Private Day Nursery Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Grass Roots Private Day Nursery Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.
- Grass Roots Private Day Nursery Ltd will make it easy for data subjects to update the information Grass Roots Private Day Nursery Ltd holds about them.
- Data should be updated as inaccuracies are discovered.

Data weeding

Data which is inaccurate or no longer relevant will be deleted or destroyed as soon as practicable. However, if required by regulatory bodies, certain data may be kept for longer periods. The length of time certain data should be kept is set out in the Data Retention Policy.

Subject access requests

All individuals who are the subject of personal data held by Grass Roots Private Day Nursery Ltd are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Ask for their data to be corrected, deleted or processing restricted.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting information, this is called a subject access request.

Subject access requests from individuals can be made either verbally or in written format to the data protection officer at Grass Roots Private Day Nursery Ltd.

The data protection officer will provide the relevant data within 30 days.

The data protection officer will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act and the GDPR allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Grass Roots Private Day Nursery Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisors where necessary.

Providing information

Grass Roots Private Day Nursery Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends the company has a Privacy Notice for staff and one for customers, setting out how data relating to individuals is used by the company.

This policy will be reviewed by management annually, who are responsible for ensuring the dissemination of this policy to all staff, volunteers and parents.