

Data Protection - Privacy Notice

Why this policy exists

This Data Protection Policy ensures HJ Lea Oakes Ltd and Oakes Millers Ltd:

- Comply with data protection law and follow 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

The Law

The Data Protection Act 1998 describes how companies must collect handle and store personal information.

The rules apply no matter how the data is stored, be that electronically, on paper or any other materials.

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

Policy Scope

The policy applies to:

- The head office of HJ Lea Oakes Ltd and Oakes Millers Ltd
- All sites of HJ Lea Oakes Ltd and Oakes Millers Ltd
- All staff and volunteers of HJ Lea Oakes Ltd and Oakes Millers Ltd
- All contractors, suppliers and other people working on behalf of HJ Lea Oakes Ltd and Oakes Millers Ltd

It applies to all data that the companies hold relating to **identifiable individuals**. This data can include:

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

Data Protection

This policy helps to protect HJ Lea Oakes Ltd and Oakes Millers Ltd from very real security risks, including:

- **Breaches of confidentiality.** E.g. information being given out inappropriately
- **Failing to offer choice.** E.g. all individuals have the right to choose how the company uses data relating to them.
- **Reputational damage.** E.g. the company could suffer if sensitive data was hacked

Responsibilities

Everyone who works for or with HJ Lea Oakes Ltd and Oakes Millers Ltd has a responsibility for ensuring the data they collect or handle is done so appropriately.

Each **team**, and **individual** within the team, that handles data must ensure that it is handled and processed in line with this policy and data protection principles.

The **Board of Directors** is ultimately responsible for ensuring that HJ Lea Oakes Ltd and Oakes Millers Ltd meet its legal obligations.

Some of these obligations are listed below:

General

- Reviewing all data protection procedures and related policies in line with an agreed schedule
- Arranging training and advice for the people covered by this policy
- Handling data protection questions from anyone covered by this policy
- Checking and approving contracts or agreements with 3rd parties that may handle the company's sensitive data

IT

- 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 3rd Party services the company is using to store and process data.

Marketing

- Approving any data protection statements attached to communications, e.g. emails and letters
- Addressing any data protection queries from the media
- Ensuring that 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 managers
- The company 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 set out here
- Strong passwords must be used and **never** shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally
- Data should be reviewed and updated if it is found to be out of date. If no longer required it should be deleted and disposed of in a safe and confidential way.
- Employees should request help from their line manager if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be stored safely.

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

The guidelines also apply to data that is usually electronically stored but has been printed out:

- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, for example 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** (CD or DVD for example) these should be kept locked away securely when not being used and encrypted if being removed from the office building.
- Data should only be stored on designated drives and servers and should only be uploaded to cloud services with the approval of a director.
- Servers containing personal data should be **backed up in a secure location** off site away from the main office location.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's backup procedures.
- Data should **never be saved directly** onto non-company laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data Use

When personal data is accessed and used it is at its greatest risk from loss or theft.

- When working with personal data, employees should ensure 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. Sensitive data must be **encrypted before being transferred electronically**.
- Employees **should not save copies of personal data to their own computers/phones**.
- It is preferred to access and update the central copy of any data rather than save it down locally.

Data Accuracy

The law requires HJ Lea Oakes Ltd and Oakes Millers Ltd to take reasonable steps to ensure that data is kept accurate and up to date. The more important the data is the more effort should be put into ensuring its accuracy.

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

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets either electronically or on paper.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- The company will make it **easy for data subjects to update the information** we hold about them.
- Data should be **updated as soon as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the sales and marketing department's responsibility to ensure the **marketing databases are checked against industry suppression files** every 6 to 12 months.

Subject Access Requests

All individuals who are the subject of personal data held by HJ Lea Oakes Ltd and Oakes Millers 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
- Be informed how the company is meeting its data protection obligations

Subject access requests from individuals should be made by email to GDPR@Hjlea.com using the access request form.

HJ Lea Oakes Ltd and Oakes Millers Ltd will aim to provide the relevant data within 40 calendar days at no cost to the individual.

We will always validate the identity of anyone making a subject access request before handing over the information.

Disclosing the data for other reasons

At HJ Lea Oakes Ltd we take your privacy very seriously and will only use your personal information to process information relevant to you as a customer, supplier or employee of the business.

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

Under these circumstances H J Lea Oakes Ltd will disclose the requested data. We will always ensure the request is legitimate and lawful.

Providing Information

HJ Lea Oakes Ltd and Oakes Millers Ltd aim to ensure that individuals are aware if their data is being processed, and that they understand:

- How the data is being used and
- How to exercise their rights under the law

To these ends the company has a privacy statement specifically setting out how data relating to individuals is used by the company.