MARLOW ROPES LTD DATA PROTECTION POLICY

The document is designed to ensure that Marlow Ropes' general terms of business are in line with data protection law and best practices. Marlow Ropes does not hold data for reasons outside of the core function of the business.

April 2018

Executive Summary

1) What information we hold and why?

All of the information that Marlow Ropes holds is directly aligned to the core function of the business and not used in any other fashion. Marlow Ropes are primarily concerned with the data protection act with regard to staffing and recruitment.

2) Are people aware of the information that we hold about them?

Marlow Ropes have addressed these issues in the following manner,

- Staffing data protection is addressed in the Data Protection Policy addendum to the company handbook.
- There is a statement included on our application form for job applications.
- Data that we hold on suppliers and customers can be considered as within the parameters of "Legitimate Interest", but is also addressed in our Privacy Statement, available on our website and emailed to relevant parties.

3) Is the information being held securely?

All personnel information in paper format is stored securely by the Managing Director, the Financial Controller (Data protection officer) and the Production Manager in a locked cabinet or cupboard.

Electronic data is securely stored and password protected in the following locations, which are all only accessible by the people detailed below:

- Employment contract database - Chairman
- Employment files – Managing Director
- Quartix Driver Tracking System – Chairman, Directors
- Sickness and absence spreadsheet – Finance Team
- Sage Payroll – Financial Controller, Payroll Administrator
- Marlow Ropes company auto enrolment scheme – Financial Controller
- Interview documents are destroyed in the event of unsuccessful applications
- All external body data (customer and supplier) is held within CRM and Accounting software.

4) Is our information up to date and accurate?

We will formally update our personal information once a year as part of the review process. In addition, the employees are aware that it is their responsibility to inform their line manager of any change in circumstances.

5) What is our deletion of data policy

Marlow Ropes will evaluate data retention after the financial year end against the parameters within this document.

6) Data placed on company website

All information placed on the company website, relevant to the data protection act, is discussed with the individuals before actioning.

7) Trained Staff

All staff members have been trained with respect to their general responsibilities regarding data protection. In addition, training has been provided to individuals dealing with specific data within the business.

- Data Protection Officer
- Finance team members involved with payroll
- Managers & Directors

8) Request for data

In the event that there is a request for data by internal or external parties then this should be channelled through the data protection officer.

9) Notification to the ICO commission

Marlow Ropes has registered with the ICO for best practice although it is felt not necessary within the core business.

Data protection policy

Context and overview

Key details

- Policy prepared by: Jon Mitchell
- Data protection officer Mark Fryer
- Approved by board / management on: 09/05/2018
- Policy became operational on: 09/05/2018
- Next review date: 01/01/2020

Introduction

Marlow Ropes Limited 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 Marlow Ropes;

- 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 Data Protection Act 1998 and the EU General Data Protection Regulations 2018 describe how organisations — including Marlow Ropes— must collect, handle and store 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 Data Protection Act 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:

- The head office of Marlow Ropes
- All branches of Marlow Ropes
- All staff and volunteers of Marlow Ropes
- All contractors, suppliers and other people working on behalf of Marlow Ropes

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
- Employee data (which is covered in a separate document as part of the overall Company handbook.)

Data protection risks

This policy helps to protect Marlow Ropes 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 Marlow Ropes has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that 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 Marlow Ropes meets its legal obligations.

- **Mark Fryer** [Data Protection Officer] 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 Marlow Ropes 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.

- **M-Tech Systems Ltd** [IT management] is responsible for:
  - 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.

- **Emma Donovan** [Marketing Manager] is responsible for:
  - 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 managers.
- Marlow Ropes **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 or IT management.

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**, such as 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:

- Marlow Ropes have no on-site servers, all data being stored a hosted cloud environment.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.
- Remote access to Company hosted servers or internet access on Company laptops or other mobile devices is **not permitted via unsecured Wi-Fi networks**.
- 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 in the secure Data Cabinet when not being used.
- Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing service**.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.

Data use

Personal data is of no value to Marlow Ropes 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 **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**. The IT manager can explain how to send data to authorised external contacts.
- 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.

- Any data sent to employees via email (such as unsolicited CV's) should be saved in the appropriate location and **securely deleted from the email account**

Data accuracy

The law requires Marlow Ropes 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 Marlow Ropes 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.** For instance, by confirming a customer's details when they call.
- Marlow Ropes will make it **easy for data subjects to update the information** Marlow Ropes holds about them.
- Data should be **updated as and when 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 marketing manager's responsibility to ensure **marketing databases are checked and updated on a regular basis.**

Subject access requests

All individuals who are the subject of personal data held by Marlow Ropes 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**.

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

Subject access requests from individuals should be made by email, addressed to the Data Protection Officer at mark.fryer@marlowropes.com. The Data Protection Officer can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged for this initial request. Further copies and excessive, unfounded or repetitive requests will be charged at £10 per request. The data controller will aim to provide the relevant data within 14 days.

The data controller 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 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Marlow Ropes will disclose requested data. However, the Data Protection Officer will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Marlow Ropes 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 statement, setting out how data relating to individuals is used by the company.

[This is available on request. A version of this statement is also available on the company's website.]