Flynn Refrigeration Ltd

Data Protection Policy

Introduction

Flynn Refrigeration Ltd will gather and use information about individuals during the practice and delivery of the business.

These individuals include customers, suppliers, business contacts, employees and other people the organisation comes in to contact with, has a relationship with or may need to contact in the future.

This policy describes how this personal data is collected, handled and stored to meet the company's data protection standards, and to comply with the Data Protection Laws and Regulations.

Purpose of the policy

The Data Protection policy ensures that Flynn Refrigeration Ltd:

- Complies with data protection laws and regulations, and follows good practice
- Protects the rights of employees, customers and partners
- Is open about how data is stored and is processed for each individual
- Protects itself from the risk of a data breach.

Data Protection Law

The Data Protection Act 1998 describes how organisations, including Flynn Refrigeration Ltd, must collect, handle and store personal information.

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

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

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

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

Data Protection - People

This policy applies to:

- The main office of Flynn Refrigeration Ltd
- All employees of Flynn Refrigeration Ltd
- All contractors, suppliers and other people working on behalf of Flynn Refrigeration.

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
- Post addresses
- Email addresses
- Telephone numbers
- Any other information relating to an individual.

Data Protection - Risks

This policy aims to help protect Flynn Refrigeration from data security risks, including:

- Breaches of confidentiality. For example, information being given out inappropriately
- Failing to provide options. For example, all individuals should be able to decide how their information is used
- Reputable damage: For example, the company may suffer if hacked and access to sensitive data is gained.

Data Protection – Responsibilities

Everyone working for and on behalf of Flynn Refrigeration Ltd has some responsibility for ensuring that data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that they do so and process it in line with this policy and data protection principles.

The following have key areas of responsibility:

- The **company directors** are ultimately responsible for ensuring that Flynn Refrigeration meets its legal obligations
- The **data protection officer** is responsible for:
    - Keeping the company directors updated about data protection responsibilities, risks and issues
    - Reviewing all data protection procedures and related policies, in line with any agreed schedules
    - Arranging data protection training and advice for the people covered by this policy
    - Handling data protection questions from employees and all those covered by this policy
    - Dealing with requests from individuals requesting to see the data Flynn Refrigeration Ltd holds about them (also referred to as ‘subject access request’)

    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The **IT manager** 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 example, cloud computer services.
- The **marketing manager** is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters
    - Addressing any data protection queries from any sources such as PR, suppliers etc.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General 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
- Flynn Refrigeration 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
- Strong passwords must be used
- Personal data must not be disclosed to unauthorised people, wither 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 data protection officer if they are unsure about any aspect of data protection.

Data Storage

This section described where and how data should be safely stored.

When data is stored on paper, it should be kept in a secure place where it can not be accessed by unauthorised people.

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 on view or where accessible to unauthorised people, for example, on the 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
- If data is stored on removable media (for example, USB/DVD), these should be kept locked away securely when not being used
- Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services
- Servers containing personal data should be sited in a secure location, away from general office space
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures
- Data should never be saved directly to laptops or other mobile devices such as tablets and smart phones
- All servers and computers containing data should be protected by approved security software and firewall.

Data Use

- When working with personal data, employees should ensure computer screens are locked when left unattended
- Personal data should not be shared informally, especially not via email, as this type of communication is the least secure
- Data must be encrypted before being transferred electronically
- 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 Flynn Refrigeration to take reasonable steps to ensure data is kept accurate and up to date.

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 example, by confirming customer details when dealing with enquiries
- Data should be updated as inaccuracies are discovered. For example, if a customer can no longer be reached on their stored number of email address, it should be removed or updated from the central database
- It is the marketing managers responsibility to ensure marketing database are checked against industry regulations throughout the year.

Subject Access Requests

All individuals who are the subject of personal data held by Flynn Refrigeration are entitled to:

- Ask what information the company holds and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how he company is meeting its data protection obligations.

If an individual requests this information from the company, they must do so in writing and will required to answer a number of identification questions.

Disclosing Data

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, Flynn Refrigeration will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the company directors and legal advisors where necessary.

Providing Information

Flynn Refrigeration 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.

A company privacy statement sets outs how data relating to individuals is being used by the company. A copy of this is available on request and is available to view on the company website.