



## Data Protection Policy

### Introduction

As a normal part of its activities CS Plumbing and Heating Limited ("The Company") has to keep personal data on employees, customers, etc. This data must be held in accordance with the requirements of the **Data Protection Act 2018**

. This policy exists to ensure CS Plumbing and Heating Limited;

- 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 individual's data;
- Protects itself from the risks of a data breach;

### Data Protections Act 2018

The **Data Protection Act 2018** describes how organisations – including CS Plumbing and Heating Limited – must collect, handle and store personal information. These rules apply regardless of whether the 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 Company must ensure that it is registered with the Information Commissioner and that it has appointed a Data Controller.

The Data Protection Act 2018 is underpinned by seven important principles. These say that personal data must:

1. Be processed fairly, lawfully and with transparency.
2. Be obtained only for specific, explicit and legitimate 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. Be processed with appropriate security measures.
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 offices held by CS Plumbing and Heating Limited.
- All staff and volunteers of CS Plumbing and Heating Limited.
- All contractors, suppliers and other people working on behalf of CS Plumbing and Heating Limited

It applies that all data that the Company holds relating to identifiable individuals, even if that information technically falls outside of the **Data Protection Act 2018**

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 CS Plumbing and Heating Limited 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 CS Plumbing and Heating Limited has some responsibility for ensuring data is collected, stored and handled appropriately. Everyone 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:

- Christopher Stocks is ultimately responsible for ensuring that CS Plumbing and Heating Limited meets its legal obligations.
  - As the data controller, Christopher Stocks, is responsible for;



- Keeping the Company staff 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 CS Plumbing and Heating Limited 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.
- Christopher Stocks in conjunction with an external web and marketing company, 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.
  - Christopher Stocks is responsible for:
    - Approving any data protection statements attached to communications such as emails and letter.
    - 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.
- CS Plumbing and Heating Limited 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 controller 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 Christopher Stocks as the data controller. 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/DVD or USB stick), 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 an approved cloud computing service.
- 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 like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

## **DATA ACCURACY**

The law requires CS Plumbing and Heating Limited 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 CS Plumbing and Heating Limited 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.
- CS Plumbing and Heating Limited will make it easy for data subjects to update the information CS Plumbing and Heating Limited holds about them. For instance, via the Company website.
- Data should be updated 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.

### **SUBJECT ACCESS REQUESTS**

All individuals who are the subject of personal data held by CS Plumbing and Heating Limited 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 in writing, addressed to the data controller. Individuals will not be charged. The data controller will aim to provide the relevant data within one month of the request. 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 2018 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, CS Plumbing and Heating Limited will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the staff members and from the Company's legal advisors where necessary.

### **PROVIDING INFORMATION**

CS Plumbing and Heating Limited 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 policy has been approved & authorised by:

Name: Christopher Stocks

Position: Managing Director

Date: May 2018