

Data Protection Policy

1st May 2018

Context and Overview

Key Details

- Policy prepared by: Victoria Saggs
- Policy became operational on: 22nd May 2018
- Next review date: 22nd May 2019

Introduction

South West Drains Limited needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the company 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 South West Drains 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 individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

The Data Protection Act 1998 describes how organisations - including South West Drains - 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 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 South West Drains
- All staff and volunteers of South West Drains
- All contractors, suppliers and other people working on behalf of South West Drains

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 South West Drains from some very real 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 South West Drains 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 (Victoria Saggs, Jason Saggs, Joseph Wood and Rebecca Wood) are ultimately responsible for ensuring that South West Drains meets its legal obligations.
- The data protection officers are responsible for:
 - ⇒ 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 any else covered by this policy.
 - ⇒ Dealing with requests from individuals to see the data that South West Drains 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 the office.
- South West Drains 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 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 officers.

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 in their company vehicle.
- Data printouts should be returned to the office, where they will be 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 monthly and never shared between employees.
- If data is stored on removable media (a cd or 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 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.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Use

Personal data is of no value to South West Drains 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.
- Data must be encrypted before being transferred electronically. All emails will be encrypted before forwarding and all messages sent via a mobile phone to engineers will be sent using WhatsApp, as this is also encrypted.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data.

Data Accuracy

The law requires South West Drains 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 South West Drains 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.
- 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 subject of personal data held by South West Drains 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 any individual contacts the company requesting this information, this is called subject access request.

Subject access requests from individuals should be made via email, addressed to the data controller at southwestdrains@live.co.uk.

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, South West Drains will disclose requested data. However the data controllers will ensure the request is legitimate.

Providing Information

South West Drains 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 upon request. A version of this statement is also available on the company's website.

Signed *V. Saggs*

Date 22 May 2018