Data Protection Policy

Produced 1st May 2018

Next Review: 1st May 2020

Introduction

Jennifer M Whittall Ltd needs to gather and use certain information about individuals.

These can include clients, 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 comply with law.

1. Why Does the Policy Exist?

This data protection policy ensures Jennifer M Whittall Ltd:

- Complies with data protection law and follows good practice
- Protects the rights of staff, clients and partners
- Is open about how it stores and processes individuals' data
- Protects itself against data breach

2. Data Protection Law

The Data Protection Act 1998 describes how organisations including Jennifer M Whittall Ltd must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or 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 6 key principles:

3. People, Risks and Responsibilities

This Policy applies to:

All employees of the company
All Associates of the company
All suppliers, contractors and people working on behalf of the company

3.1 Data Protection Risks

This policy helps to protect Jennifer M Whittall Ltd 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 successful gain access to sensitive data.

3.2 Responsibilities

Everyone who works for Jennifer M Whittall Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

4. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to RP Business Support/Leegomery Computers.

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.
- Staff and Associates should make sure paper and printouts are not left where unauthorised people could see them, like on a printer, on a public table.
- Printouts should be shredded and disposed of securely when no longer required. Please refer to Data Retention Policy.

When data is stored electronically it must be protected from unauthorised accidental deletion, and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between staff and/or Associates.
- If data is stored on removal media (like USB), these should be kept locked away securely when not being used.
- Data should only be stored on designated drivers and servers and should only be uploaded to an approved cloud computing service (i.e. office 365).
- Data should be backed up frequently.
- All servers and computers containing data should be protected by approved security software and a firewall.

5. Data Use

Personal data is no value to Jennifer M Whittall Ltd 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:

- Data must be encrypted before being transferred electronically
- Personal data should never be transferred outside of the European Economic Area.

- Staff and Associates should not sae copies of personal data to their own computers.
- When working staff and Associates must ensure their screens are locked if unattended.

6. Data Accuracy

The law requires Jennifer M Whittall Ltd 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 Jennifer M Whittall Ltd should put into ensuring its accuracy.

Reasonable steps to ensure it is kept accurate and up to date as possible by:

- Holding data in as few places as possible.
- Take every opportunity to ensure data is updated.
- Jennifer M Whittall Ltd will make it easy for data subjects to update the information held.
- Any inaccuracies discovered updated.

7. Subject Access Requests

All individuals who are the subject of personal data held by Jennifer M Whittall Ltd are entitled to:

- Ask what information is held 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 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 Controller at jenny@jmw-ltd.co.uk. The Data Controller can supply a standard request form, although individuals do not have to use this.

The Data Controller will aim to provide the relevant data within 14 days.

The Data Controller will always verify the identify of anyone making a subject access request before handing over any information.

8. 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 Jennifer M Whittall Ltd will disclose requested data, however, the Data Controller will ensure the request is legitimate.

9. Providing Information

Jennifer M Whittall Ltd 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 contained within the client consent form.