

Data protection policy

Context and overview

Key details

- Policy prepared by: Jo Permaul
- Policy became operational on: May 25th 2018
- Next review date: May 25th 2019

Introduction

Jo Permaul needs to gather and use certain information about individuals in order to complete consultations.

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 Jo Permaul:

- Complies with data protection law and follow good practice
- Protects the rights of, 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 Jo Permaul— 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:

- All contractors, suppliers and other people working on behalf of Jo Permaul

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 Jo Permaul 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

Jo Permaul has responsibility for ensuring data is collected, stored and handled appropriately.

- 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.
 - Ensure marketing initiatives abide by data protection principles.
- Personal data **will not be disclosed.**

- 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.

Data storage

When data is **stored on paper**, it will be kept in a secure place where unauthorised people cannot see it.

- Paper or files will be kept **in a locked drawer or filing cabinet**.
- Electronic data is password protected.

Data accuracy

The law requires Jo Permaul to take reasonable steps to ensure data is kept accurate and up to date.

Subject access requests

All individuals who are the subject of personal data held by Jo Permaul 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 controller at [email address]. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access 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, Jo Permaul will disclose requested data.

Providing information

Jo Permaul 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