

Data protection policy

Context and overview

Key details

Policy prepared by: Helen Pilkington

Policy became operational on: 07/05/2022.

Next review date: 07/05/2025

Introduction

In the Room Counselling needs to gather and use certain information about individuals. 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 In the Room Counselling:

- Complies with data protection law and follow 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 In the Room Counselling, 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.

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 In the Room Counselling 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 In the Room Counselling has some responsibility for ensuring data is collected, stored and handled appropriately.

Every person 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 director is ultimately responsible for ensuring that In the Room Counselling meets its legal obligations.
- The data protection officer, Helen Pilkington, is responsible for:
 - Keeping the company up to date 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 In the Room Counselling 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.