



Data Protection Policy

Rising Hope Counselling
Rachel Herbert MBACP
Sole Trader

1. Purpose of This Policy

Rising Hope Counselling is committed to protecting the privacy, dignity, and confidentiality of all clients. This policy explains how personal data is collected, stored, used, and protected in accordance with:

- The **UK General Data Protection Regulation (UK GDPR)**
- The **Data Protection Act 2018**
- The **BACP Ethical Framework for the Counselling Professions (2018)**

This policy reflects the ethical principles of **trustworthiness, autonomy, beneficence, non-maleficence, justice, and self-respect**, which underpin my counselling practice.

2. Data Controller

The data controller is:

Rachel Herbert MBACP
Rising Hope Counselling
Sole Trader

I am responsible for ensuring that personal data is processed lawfully, ethically, and transparently.

3. ICO Registration



Rising Hope Counselling is registered with the **Information Commissioner's Office (ICO)** as a data controller. **ICO Registration Number: ZB683181**

Client data is processed in accordance with ICO guidance and UK data protection law.

4. Types of Personal Data Collected

I may collect and hold the following personal data:

- Name, address, email address, telephone number
- Date of birth
- Emergency contact details
- GP details (where relevant)
- Assessment information and risk assessments
- Session notes and clinical records
- Payment and invoicing records
- Correspondence via email, text, or telephone

Some information may be considered **special category data**, including mental health information, physical health details, sexuality, ethnicity, or trauma history, where this is relevant to therapeutic work.

Only data that is **necessary and proportionate** to the provision of counselling is collected, in line with the BACP principle of **respect for client autonomy and privacy**.

5. Lawful Basis for Processing

Personal data is processed under one or more of the following lawful bases:

- **Contract** – to provide counselling services
- **Consent** – particularly for special category data
- **Legal obligation** – including safeguarding responsibilities
- **Vital interests** – where there is risk of serious harm
- **Legitimate interests** – for safe, ethical therapeutic practice



In line with the BACP Ethical Framework, consent is **informed, ongoing, and reviewed**, and clients are informed of the limits of confidentiality at assessment.

6. Confidentiality and Ethical Practice

Confidentiality is central to the therapeutic relationship and is maintained in accordance with the **BACP Ethical Framework**.

Information may be shared without consent only when:

- There is a serious risk of harm to the client or others
- Safeguarding concerns arise involving children or vulnerable adults
- There is a legal requirement (e.g. court order)
- Information is discussed in **clinical supervision** (anonymised where possible)

Wherever possible, clients will be informed before any disclosure is made, reflecting the ethical principles of **trust, transparency, and non-maleficence**.

7. Storage and Security of Data

I take all reasonable steps to ensure data is stored securely:

- Paper records are kept in a locked filing cabinet
- Electronic records are password-protected and encrypted
- Devices used for client data have appropriate security measures
- Emails and digital communications are handled with care
- Only I have access to identifiable client records

This reflects my ethical responsibility for **self-respect and professional integrity**.

8. Retention of Records

Client records are retained for:



- **7 years after the end of therapy** for adults
- **Until age 25** for children and young people

This is in line with professional, ethical, and insurance guidance. Records are securely destroyed once the retention period ends.

9. Client Rights

Clients have the right to:

- Access their personal data
- Request correction of inaccurate information
- Request erasure of data (where legally and ethically appropriate)
- Restrict or object to processing
- Withdraw consent
- Make a complaint to the **Information Commissioner's Office (ICO)**

Requests should be made in writing and will be responded to within one calendar month.

10. Data Breaches

Any data breach will be managed promptly and responsibly. Where required, breaches will be reported to the ICO within **72 hours**, and clients will be informed if there is a risk to their rights or freedoms.

11. Review of This Policy

This policy is reviewed annually, or sooner if legislation, ethical guidance, or practice arrangements change.

Last reviewed: January 2026

Next review due: January 2027