Data Protection Policy

REVISION RECORD

Version	Description	Date
3	Third draft	December 2025

Signed:

Director

Policy Principles

Personal and Sensitive Information

Any personal information held by Wye Dean Wellbeing must be treated as confidential and must not be shared without the individual's consent. In counselling and therapeutic work, there may be circumstances where information is shared without consent, such as where there are safeguarding concerns or serious risks to mental health.

Personal and sensitive information is defined as any information held in a professional capacity that enables a person's identity to be established. This may include, but is not limited to, name, date of birth, address, NHS number, or other identifying details. Combinations of information, such as postcode and date of birth, may also be sufficient to identify an individual and must be treated accordingly.

The loss, misuse, or misdirection of sensitive or confidential information can have a significant impact on individuals. Under **UK GDPR and the Data Protection Act 2018**, personal data includes information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, physical or mental health conditions, sexual life or sexual orientation, criminal offences or allegations, and the outcomes of related proceedings. Financial information and commercially sensitive security arrangements are also included.

Treatment/Counselling

Everyone has the right to privacy and confidential treatment, including counselling and psychotherapy, without disclosure to others.

A practitioner may encourage a client to seek additional help or support during therapy; however, this may not always be safe or appropriate. Such decisions must be made collaboratively and with respect for the client's circumstances and wishes.

Confidentiality is fundamental to the development of the therapeutic alliance. Material discussed during counselling sessions is therefore confidential, subject to legal and ethical limits, and is protected under the **Human Rights Act 1998**.

At the start of therapy, a written contract will be agreed between the counsellor and the client outlining confidentiality, its limits, and associated risks.

Information Sharing

Information may be shared without consent only where legally or ethically required, including:

- Where there is a risk of serious harm to the individual or others
- Where there is a disclosure or suspicion of abuse
- Where there are concerns relating to serious criminal activity (e.g. terrorism, drug trafficking, proceeds of crime, fraud)
- Where counselling records are lawfully required or ordered by a court

Wherever possible, counsellors will seek informed consent before sharing information. Only information that is necessary, proportionate, and relevant to the concern will be shared, and non-essential sensitive information will be excluded.

Information Sharing – Data Security

Any communication containing confidential or personally identifiable information (such as name, date of birth, or address) will be sent via secure and encrypted systems.

Information and Storage Security

In accordance with **UK GDPR and the Data Protection Act 2018**, informed consent will be obtained when contracting with clients for the storage and processing of personal records. All feedback, evaluation material, and client records will be stored electronically on a password protected with 2-factor authentication database. A client's record will be archived when they have completed their treatment and counselling plan.

Client Access to Records

Under **UK GDPR and the Data Protection Act 2018**, clients have the right to request access to their counselling records, subject to legal and ethical considerations.

Basic Data Protection Guidance

- Always verify the identity of the person you are communicating with.
- Never disclose personal data in order to confirm someone's identity. Identity checks should be completed by asking the individual to confirm known information (for example, their address, DOB).

Data Breach Incident Management

Any data breach, whether actual or suspected, must be reported immediately to a Director of Wye Dean Wellbeing, who will notify the designated Data Protection lead. This will initiate an investigation and, where required, reporting to the Information Commissioner's Office (ICO) in line with legal obligations.

Breach of Policy

Failure to manage information securely may place Wye Dean Wellbeing at risk of non-compliance with UK GDPR and the Data Protection Act 2018. All individuals working for, or on behalf of, the organisation share a collective responsibility for protecting personal and confidential information. Any failure to comply with this policy may result in appropriate action being taken, which may include disciplinary procedures.