



Privacy Policy (GDPR Compliance)

Our Privacy Policy covers the collection and disclosure of personal information that may be collected by us and passed onto our partners who need the information to carry out their job roles. We do not share our information with other agencies but we only pass onto third parties who need the information to carry out their job role to protect the clients.

The following Data Protection Promise describes how we collect and use personal information about you in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018. We are committed to protecting the privacy and security of your personal information at all times.

We will comply with data protection law when it comes to the processing of your data. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

1. Introduction

1.1 Rupaal is committed to good practice in all aspects of service delivery and employment practice.

1.2 A clear policy on confidentiality is essential to safeguard individual clients and to ensure high standards of practice.

1.3 No policy can cover every situation but this policy provides a framework within which it is essential for staff to exercise a high level of accountability and professional judgement.

2. Basic Principles of Client Confidentiality

2.1. All information relating to clients must be treated with utmost respect. In many cases, clients divulge information which may be sensitive and painful. Clients may feel very vulnerable if this information is not treated with respect.

2.2. The principles of "**informed consent**" and "**need to know**" are the basis of Rupaal's confidentiality policy.

i. *Informed Consent*

Since all information divulged by clients must be treated with respect, it is important to establish with the client if this information may be passed on to anyone else. Wherever possible, permission to share information must be sought from the individual client concerned.

ii. Need To Know

Information given by a client to a member of staff should only be passed on to someone else where there is a legitimate *need to know* in order to deliver a service to the person.

2.3. In practice, there are exceptional circumstances where information will need to be shared with other agencies against the expressed wishes of the client.

For example:

- A client's life is considered to be at risk
- Other people's lives are considered to be at risk
- It is a requirement of a court order
- It is a requirement of law
- It is in the public interest

2.4. All staff should be able to share all relevant information on case work and work in progress with their line manager. The need for both formal and informal supervision is essential for both accountability and staff support. Clients should be made aware that key workers involved in their care and support will need to discuss their involvement with their line manager.

2.5. The main public interest justification for the disclosure of health information are as follows (based on Department of Health Guidance 1994):

- For public accountability and monitoring purposes
- Serious risks to the health of other individuals
- Serious risk to public health
- The reporting of adverse drug reactions
- The prevention, detection or prosecution of serious crimes
- Disclosures to professional regulatory bodies (e.g. investigations of professional mis-conduct)
- Bona Fide and approved clinical and scientific research and surveys

2.6. Any requests for information from an external agency on the grounds of public interest should be treated with care, discussed with senior managers and fully documented. Depending on the nature of the request and the information requested, it may be necessary to arrange a review meeting with the relevant agencies involved.

2.7. Where a request for disclosure is made in relation to a serious crime, the following conditions must be satisfied.

- The crime must be sufficiently serious for the public interest in disclosure to prevail over the individual's right to confidentiality

- It must be established that without the disclosure the task of preventing or detecting the crime would be seriously prejudiced or delayed

2.8. Disclosure of Information in Respect of Abuse or Supply of Illegal Drugs

In line with Point 2.3, the disclosure of information to the police in order to comply with Rupaal's Use or Supply of Illegal Drugs, Corporate Policy, is permissible with or without the expressed permission of the client. If such information is to be shared this should only be done in consultation with the Senior Manager.

2.9. Protection of Children and Vulnerable Adults

In the event of a worker being made aware of information relating to possible or actual physical, sexual, financial or emotional abuse of children or vulnerable adults, they should report their concerns immediately to their line manager and the relevant Service Director or senior on-call manager. Their concerns will be dealt with within the agreed Child Protection Policy or Vulnerable Adults Policy, devised by the Social Services Department in the relevant Local Authority. Reference should also be made to Rupaal's Child Protection Policy and Adults at Risk Policy and the safety of children and vulnerable adults should always be given the highest priority and should override considerations of confidentiality.

2.10. If any member of staff feels that any of the situations outline in 2.7 or 2.8 apply, then it is essential that they discuss the matter with their Line Manager, Duty Manager, or any other senior member of staff.

3. Case Files

3.1. Rupaal will establish an individual case file for each client. Files must be kept up to date and relevant, ensuring that each entry is signed dated.

3.2. Every client has an established case file, which the member of staff is responsible for establishing and maintaining. Files must be kept up to date and relevant, giving clear dates and the signature of the staff member making the entry.

3.3. Staff should avoid taking client files out of the office. In unusual circumstances client files may be removed with the prior agreement of the Service Manager. In such cases files should be booked out giving the name of the person taking the file, the client's name and expected date of return. If removing a file copies of the yellow front sheets detailing essential information should be retained in the file hanger, so that staff working with the client will have access to such information in the event of an emergency.

4. Your rights –

4.1 Right to Access – this means that you can ask us for a copy of all personal data we hold about you. This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

4.2 Correction Right – if you believe that any of the information we hold about you is incorrect or out of date, you have the right to correct such information by providing us with the correct up to date information. In addition, you can ask us to delete the incorrect or out of date information and we will be happy to do so unless we are prevented from doing so by law or regulation.

4.3 Right to be forgotten – this enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it.

4.4 Right to Restrict Processing – in some limited circumstances you have the right to restrict the processing of your data.

4.5 Right of Objection to Processing – you have the right to object to us using your data for direct marketing purposes and to profiling.

4.6 Right of Data Portability – you have the right to request a copy of the personal data we hold about you in a commonly used and machine-readable format. We can provide your data either to you or to such other third party as you specify in your request.

4.7 Automated Decision-Making Objection Right – automated decision-making is where a decision is made entirely by technological means without human intervention. We don't use or rely on automated decision-making.

5. What do we collect and where do we collect it from?–

5.1 We collect our data from staff, clients, client's relatives and our partners from the local authorities. We may collect the following information from you:

- Name/s
- Contact information including email address, phone numbers
- Demographic information such as postcode, preferences and interests
- Generally, health information we collect about you includes:
- Your previous and current medical history (including, where clinically relevant, a family medical history) and details of treatment and health services you have received
- Your care plan
- Medications you take
- Information about other healthcare professionals and health service providers who are involved in your care
- Information about your healthcare preferences and wishes
- Your attorney, guardian or other person responsible for your healthcare decisions