Data Protection Policy

---

1. Purpose

The purpose of this Data Protection Policy is to ensure that our organisation processes personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy outlines how we collect, use, store, share, and protect personal data.

2. Scope

This policy applies to:

- All employees, contractors, volunteers, and third parties working on behalf of the organisation
- All personal data processed by the organisation, whether stored electronically, on paper, or in any other format

3. Definitions

- **Personal Data**: Any information relating to an identified or identifiable individual.
- **Special Category Data**: Sensitive data requiring additional protection (e.g., health data, ethnicity, biometric data).
- **Processing**: Any operation performed on personal data, including collection, storage, use, sharing, or deletion.
- **Data Subject**: The individual whose personal data is being processed.
- **Data Controller**: The organisation determining how and why personal data is processed.
- **Data Processor**: A third-party processing data on behalf of the controller.

4. Data Protection Principles

We commit to processing personal data in accordance with the following principles:

1. **Lawfulness, fairness, transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Accuracy**
5. **Storage limitation**
6. **Integrity and confidentiality**
7. **Accountability**

5. Lawful Basis for Processing

We will only process personal data when at least one lawful basis applies, such as:

- Consent
- Contractual necessity
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Special category data will only be processed under an additional lawful condition.

6. Data Collection and Use

We will:

- Collect only the minimum data necessary
- Inform individuals about how their data will be used
- Use data only for the purposes for which it was collected
- Keep data accurate and up to date

7. Data Storage and Security

We will ensure that personal data is stored securely by:

- Using password protected systems and encrypted storage
- Restricting access to authorised personnel only
- Implementing physical security measures for paper records

- Regularly reviewing security controls

8. Data Sharing

Personal data will only be shared when:

- Required by law
- Necessary for business operations
- The data subject has given consent
- Appropriate data sharing agreements are in place

We will ensure that all third-party processors comply with UK GDPR requirements.

9. Data Retention

Personal data will be retained only for as long as necessary for the purposes for which it was collected. Retention periods will be defined in the organisation's Data Retention Schedule. Data will be securely deleted or anonymised when no longer required.

10. Data Subject Rights

Individuals have the right to:

- Access their personal data
- Rectify inaccurate data
- Request erasure ("right to be forgotten")
- Restrict processing
- Object to processing
- Data portability
- Withdraw consent at any time

Requests will be handled within statutory timeframes.

11. Data Breaches

All data breaches must be reported immediately to the designated lead. We will:

- Investigate all breaches
- Maintain a breach log
- Notify the ICO within 72 hours when required

- Inform affected individuals when there is a high risk to their rights and freedoms

12. Roles and Responsibilities

- **Senior Management**: Ensures compliance and provides resources and oversees data protection strategy and compliance
- **Employees**: Must follow this policy and complete data protection training

13. Training and Awareness

All staff will receive regular data protection training appropriate to their role.

14. Policy Review

This policy will be reviewed annually or when significant changes occur in legislation or organisational practices.

Approved by: Rony Managing Director

OPT HEALTHCARE LIMITED