Data protection Policy

Person Responsible	**Operations Manager**
Author	**Denise McGregor**
Issue Date	**March 2023**
Review Date	**March 2026**
Approved by	**SMT**

DOCUMENT HISTORY

Date	Author/Editor	Summary of Changes	Version No.
02.03.2020	Robert Krawczyk	New policy	1.0
04.03.2023	Denise McGregor	Review	2.0

Please note that the only valid version of the policy is the most recent one. Whilst this document may be printed, the electronic version posted on the main drive is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the main drive.

CONSULTATION AND RATIFICATION SCHEDULE

Name of Consultative Body	Date of Approval
Senior Management Team	02.03.2020
Senior Management Team	04.03.2022

CROSS REFERENCE TO OTHER POLICIES/STRATEGIES

This policy should be read in conjunction with:	Detail

Contents

.

1.0 Primecare Health LTD Values

Primecare Health LTD are true to the core purpose of our organisation and the services we deliver.

Working within these values will guide and deliver our vision and mission of Primecare Health Ltd.

LIKE IT….

Listen – always with interest, concern and action

Inspire – through every interaction so people can achieve their ambitions

Kind – genuine care and compassion

Excellence – by striving to be the best we can

Integrity – acting ethically and being accountable

Trusting – rely upon us to do what we say we will do

2.0. Introduction

Primecare Health Ltd is obliged to comply with the Data Protection Act 1998. The Information Commissioner who oversees compliance and promotes good practice, requires all data controllers who process personal data to be responsible for their processing activities and comply with the eight data protection principles of 'good information handling'. This document sets out Primecare Health Ltd policy and controls in compiling with its statutory obligations.

3.0. Purpose

The purpose of this policy is to:
Ensure that Primecare Health Ltd follows and adheres to all GDPR's laws and regulations in line with the legislation laid out by the Government of the United Kingdom.
Establish a standardised approach ensure that GDPR protocols are met across all services.
Outline the responsibilities of staff members involved when handling personal data.
Ensure data privacy and confidentiality in the collection and analysis of outcomes.
This information includes but is not limited to that all personal data must.

-]Be processed fairly and lawfully
- Be obtained only for specified and lawful purposes, and not be processed in any incompatible manner
- Be adequate, relevant and not excessive
- Be accurate and, where necessary, kept up to date
- Not be kept longer than necessary
- Shall be processed in accordance with the rights of Data Subjects
- Be protected by appropriate security measures

This policy applies to all personal data held by Primecare Health Ltd. It encompasses manual/paper records and personal data electronically processed including information gathered on our office CCTV system.
The obligations outlined in this policy apply to all those who have access to personal data held by Primecare Health Ltd.

Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or is deliberately acting outside of their recognised responsibilities may be subject to the Company's disciplinary procedure, including dismissal where appropriate. All individuals permitted to access personal data in line with their work duties must agree to comply with this policy and agree to undertake any relevant training that may be appropriate to the job/position being undertaken.

4.0 Definitions

Data: Any information that is: -

- Being processed by means of equipment operating automatically in response to instructions given for that purpose.
- Recorded with the intention that it should be processed by means of such equipment (e.g., CD ROM)
- Recorded as part of a manual filing system or with the intention that it should form part of a relevant filing system.

Personal Data: Personal data is defined as, data relating to a living individual who can be identified from:

- That data.
- That data and other information, which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive Personal Data: Sensitive personal data is defined as personal data consisting of information as to racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; or criminal proceedings or convictions.

Data Subject: An individual who is the subject of the personal data.

Processing: any activity/operation performed on personal data - whether held electronically or manually, such as obtaining, recording, holding, disseminating, or making available the data, or carrying out any operation on the data. This includes organising, adapting, amending, and processing the data, retrieval, consultation, disclosure, erasure, or destruction of the data. It is difficult to envisage any activity, which does not amount to processing.

Information Commissioner: an independent Officer appointed to oversee the implementation of the Data Protection legislation.

Relevant filing system: means any filing system with an index.

5.0 Policy Statement

In order to operate efficiently, Primecare Health Ltd has to collect and use information about individuals. This may include present, current, past, and prospective employees, individuals and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government and other bodies. This personal information will be handled and dealt with properly, however it is collected, recorded, and used, and whether it be on paper, in computer records or recorded by any other means.

Primecare Health Ltd regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Company and those with whom it carries out business. Primecare Health Ltd will ensure that it treats personal information lawfully and correctly. Primecare Health Ltd fully endorses and will adhere to the Principles of Data Protection as set out in the Data Protection Act 1998. Disciplinary or other action may be taken against any employee or member who breaches any aspect of this policy or the procedures for its implementation.

Overall responsibility for the efficient administration of the Data Protection legislation lies with the Company Director.

6.0 General Principles

The Data Protection Act stipulates that anyone processing personal data must comply with the Eight Principles of good practice. These Principles are legally enforceable.

The principles require that personal information:

- Shall be processed fairly, lawfully, and in particular, shall not be processed unless specific conditions are met.

- Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is processed.
- Shall be accurate and where necessary, kept up to date.
- Shall not be kept for longer than is necessary for that purpose or those purposes.
- Shall be processed in accordance with the rights of data subjects under the Act.
- Shall be kept secure i.e., protected by an appropriate degree of security.
- Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of data protection.

7.0 Confidentiality and Security
Personal data is confidential, and confidentiality must be preserved in compliance with the Data Protection Principles. Confidential information can be the most valuable asset of a business and employees will automatically have duties to their employers to ensure that confidential information is not knowingly or recklessly misused. Accordingly, where personal data is stored in -

- Manual files (paper records) - access must be restricted solely to relevant staff and stored in secure locations (e.g., lockable cabinets), to prevent unauthorized access.
- Electronic files - Computer systems will be configured, and computer files created with adequate security levels to preserve confidentiality. Those who use the Company's computer equipment will have access only to the data that is both necessary for the work they are doing and held for the purpose of carrying out that work.

At certain times it may be required that personal data be disclosed under one of the exemptions within the Data Protection Act 1998. If there is a requirement for this an audit trail will need to be kept to provide accurate records of any disclosures of personal data.

8.0 Processing data
All processing of personal data will comply with the Data Protection Principles. In the situation where a third party processes data, the third party will be required to act in a manner which ensures compliance with the Data Protection Act 1998 and has adequate safeguards in place to protect the personal data.

Data will only be processed for the purpose for which it was collected and should not be used for additional purposes without the consent of the data subject.

The Company will endeavour to inform all individuals of why their personal data is being collected. In line with the first data protection principle, all information will be collected fairly and lawfully and processed in line with the purpose for which it has been given.

The Company will remember that when collecting data via the telephone or face to face the above information should also be made clear to the data subject before any processing of their personal data takes place.

Personal data must not be disclosed, except to authorised users, other organisations and people who are pre-defined as a notified recipient or if required under one of the exemptions within the Data Protection Act 1998.

9.0 Data Subject Rights

The Right of Subject Access (section 7 to 9)
A written request received by Primecare Health Ltd from an individual wishing to access their rights under the provisions of the Data Protection Act 1998 is known as a Subject Access Request. Sections 7 to 9 of the Act gives an individual the rights to request access to any 'personal data' that they believe may be held about them.

If it does hold the requested information, then it will provide a written copy of the information held about them and details of any disclosures which have been made. The information requested will be provided promptly and in any event within 40 calendar days of receipt of the subject access request. If the information cannot be disclosed within the time period specified, the data subject will be kept fully informed of the process and given access to any personal data that may already have been gathered.

A fee of £10 will be charged for the provision of any personal data held by Primecare Health Ltd to a data subject.

If the data subject believes that Primecare Health Ltd has not responded correctly and are not happy with the Company's response to their concerns they are able to complain to the Information Commissioner.

Prevention of Processing Causing Damage or Distress (s10)
If an individual believes that a data controller is processing personal data in a way that causes them substantial unwarranted damage or substantial unwarranted distress, they can send a notice (data subject notice) to the data controller requesting, within a reasonable time, the data controller to stop the processing.

Right to Prevent Processing for Purposes of Direct Marketing
An individual is entitled to request (in writing) a data controller to cease, or not to begin, processing their personal data for the purpose of direct marketing. When a data controller receives a written notice, they must comply as soon as practically possible.

An individual may apply to a Court for an order if the data controller fails to comply with a written notice.

Rights in relation to automated decision taking (section 12)
An individual is entitled, by written notice, to require a data controller to ensure that no decision, which significantly affects that individual, is based solely on the processing, by automatic means, of personal data of which that individual is the data subject.

Right to compensation (section 13)
An individual who suffers damage, or damage and distress, as the result of any contravention of the requirements of the Act by a data controller, is entitled to compensation where the data controller is unable to prove that they had taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

Dealing with inaccuracy (section 14)
A data subject may apply to the Court for an order requiring the data controller to rectify, block, erase or destroy such data relating to that data subject as are inaccurate together with any other personal data relating to the data subject which contain an expression of opinion which the Court finds is based on the inaccurate data.

Monitoring, review and evaluation
This policy will be reviewed and updated annually, or as and when current legislation changes.

10.0 Rights of Access:

Service Users and employees have the right to be supplied with a copy of their personal data the company retains. All requests are to be made to the Registered Manager who is the - "Data Protection Co-ordinator". In their absence the company's responsible individual is to be contacted. An authorised representative may be allowed to view the data provided the Registered Manager or Responsible individual is satisfied that permission has been given.

The company will respond to any request for personal data within ten days.

Viewing of the document/s will be in the presence of the Registered Manager or responsible individual. This is for security reasons i.e. so that no material can be removed or destroyed.

Service Users and employees are requested to inform the company of any changes in their circumstances that could affect the accuracy of the data.

Every effort will be made to resolve any disagreement between the company and the data subject, but in situations where the matter cannot be resolved, the following procedures are to be followed:

Service Users are requested to use the company's formal complaints procedure.

Employees are requested to use the company's formal grievance procedure.

11.0 RETENTION OF RECORDS

Service User Records:

Service User records covered by this policy shall be retained, after the actual date of the Service User leaving for the following period – 5 years, after that period the records will be destroyed.

What may Service User records contain?

They may contain any information legitimately required for the purposes of:

Statutory records required by legislation, regulations or at the request of the registration authority.
Operational management and administration that will enable the company to give quality care

These may include the following:

- Service User Agreement
- Service User Assessment Details
- Service User Care Plan
- Service User Financial Account
- Service User Medical Records (Depending on Circumstances)
- Risk assessment forms associated with the Service User
- Reports from Support Staff
- Correspondence with family members and other care professionals.

These are examples only and there will be other legitimate entries that may be included.

What may not be included is information, data or other material that cannot legitimately be shown to be related directly or indirectly to affording the Service User quality care.

Record Review:

Records may be reviewed and out of date and irrelevant data will be destroyed securely by shredding.

12.0 Security

Paper data that is no longer to be kept must be destroyed by means of a shredder. In the event of the scrapping of a computer, the hard drive must be erased by means of software that overwrites the hard drive to the extent that it is impossible to recover the data. A copy of such software is available from the Registered Manager.

No member of staff may remove service user or employee data (paper or electronic) from the organisation unless expressly permitted to do so by a senior member of staff.