YOU IN MIND
(Home Care) Ltd

You in Mind (Homecare) Limited CONFIDENTIALITY POLICY

You In Mind (Homecare) Limited hereinafter referred to as 'the Organisation' is committed to providing a confidential service to its users. No information given to the Organisation will be shared with any other organisation or individual without the user's expressed permission.

For the purpose of this policy, confidentiality relates to the transmission of personal, sensitive or identifiable information about individuals or organisations (confidential information), which comes into the possession of the Organisation through its work.

The Organisation holds personal data about its staff, users, members etc which will only be used for the purposes for which it was gathered and will not be disclosed to anyone outside of the organisation without prior permission.

All personal data will be dealt with sensitively and in the strictest confidence internally and externally.

Purpose

The purpose of the Confidentiality Policy is to ensure that all staff, members, volunteers and users understand the Organisations requirements in relation to the disclosure of personal data and confidential information.

Principles

- All personal paper-based and electronic data must be stored in accordance with the Data Protection Act 1998 and General Data Protection Regulations (GDPR) and must be secured against unauthorised access, accidental disclosure, loss or destruction.

- All personal paper-based and electronic data must only be accessible to those individuals authorised to have access, including the data subject.

Statistical Recording

The Organisation is committed to effective statistical recording of the use of its services in order to monitor usage and performance.

All statistical records given to third parties, such as to support funding applications or monitoring reports for the local authority shall be produced in anonymous form, so individuals cannot be recognised.

Records

All records are kept in locked filing cabinets. All information relating to service users will be left in locked drawers. This includes notebooks, copies of correspondence and any other sources of information. In relation to document's used and stored within the service user's own home, as required with domiciliary care, all records will be stored as preferred by the individual.

Personal information relates to any information which can identify an individual and some confidential details about them. All information will be collected for the purposes of delivering safe, effective and appropriate care and support and will be stored and handled in a secure manner with the consent of the individual or person acting on their behalf.

The personal information we will collect includes:

- Name, address, telephone, email and other contact details;
- Date of Birth;
- Next of Kin or emergency contact details;
- Medical information including GP details, medical condition, background and health needs, medication and dosage;
- Religion and cultural information and ethnicity;
- Dietary requirements and preferences;
- Risk and assessment needs;
- Kay safe codes;
- Financial information for invoicing and payments

The reasons we request your information and the things we use this for include:

- Assessing your care and support needs;
- Managing your care and support and ensuring that we continue to meet your needs appropriately;
- Managing your information and ensuring that data we hold remains accurate, up to date, appropriate and with your consent;
- Managing data and continuing compliance with data laws, legislation and other relevant guidance;

- Compliance with guidance set out by CQC and other governing bodies;
- Invoicing and financial purposes

There may be occasions when we need to share personal data for the purpose of safely delivering or arranging care, to keep you safe or where there is immediate danger to yourself or others. Information will also need to be shared where there has been a crime committed or we are required by law to do so. The people we will need to share your information with include:

- Medical professionals such as GP, Nurse, Paramedics, Consultants etc;
- Police and other emergency services;
- Local Authority;
- CQC;
- Regulatory bodies and Health and Safety Executive;
- Software system providers

Any information shared will be done so in your best interests and for the purposes of safeguarding.

Breaches of Confidentiality

The Organisation recognises that occasions may arise where individual workers feel they need to breach confidentiality. Confidential or sensitive information relating to an individual may be divulged where there is risk of danger to the individual, a volunteer or employee, or the public at large, or where it is against the law to withhold it. In these circumstances, information may be divulged to external agencies e.g. police or social services on a need to know basis.

Where a worker feels confidentiality should be breached the following steps will be taken:

- The worker should raise the matter immediately with their Line Manager.

- The worker must discuss with the Line Manager the issues involved in the case and explain why they feel confidentiality should be breached and what would be achieved by breaching confidentiality. The Line Manager should take a written note of this discussion.

- The Line Manager is responsible for discussing with the worker what options are available in each set of circumstances.

- The Line Manager is responsible for making a decision on whether confidentiality should be breached. If the Line Manager decides that confidentiality is to be breached then they should take the following steps:

The Line Manager should contact the Registered Manager in the first instance, or Deputy Manager where applicable. The Manager should review the full facts of the case and make a decision as to whether confidentiality should be breached. Where required the Registered Manager may seek guidance from CQC or local authority on the case ensuring they do not breach confidentiality in doing so. The Line Manager should seek authorisation to breach confidentiality from the Registered Manager.

If the breach confidentiality is agreed, a full written report on the case should be made and any action agreed undertaken. The Line Manager is responsible for ensuring all activities are actioned.

Legislative Framework

The Organisation will monitor this policy to ensure it meets statutory and legal requirements including the Data Protection Act, GDPR, Children's Act, Rehabilitation of Offenders Act and Prevention of Terrorism Act. Training on the policy will include these aspects.

Ensuring the Effectiveness of the Policy

All Executive Committee members will receive a copy of the confidentiality policy. Existing and new workers will be introduced to the confidentiality policy via induction and training. All service User's will be made aware of the policy on commencement of their care contract. The policy will be reviewed annually and amendments will be proposed and agreed by the Executive Committee.

Non-adherence

Breaches of this policy will be dealt with under the Grievance and/or Disciplinary procedures as appropriate.