Title of Policy:	**Data Protection - Clients**
Section:	**Human Resources**

Purpose

This policy details the Company's legal obligation to protect Clients' confidential information and personal data.

Statement

Aim and scope of policy

This policy applies to the processing of personal data in manual and electronic records kept by the Company in connection with its main purpose which is the provision of personal care services within the local community it serves.

It also covers the Company's response to any data breach and other rights under the General Data Protection Regulation.

This policy applies to the personal data of the Clients who have sought and or agreed to the Company providing personal care services.

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Procedure and Guidance

The Company makes a commitment to ensuring that personal data, including special categories of personal data is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. In line with GDPR, the Company understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Types of data held

Personal data is kept in Client files or within the Company's Operations management systems. The following types of data may be held by the Company, as appropriate, on relevant individuals:

- Full name;
- The name the Client likes to be called;
- Address;
- Telephone Number(s);
- Email address, if available;
- Date of Birth;
- Nationality;
- Relationship status (e.g. married, divorced etc.);
- Whether the Client lives alone;
- If not, the name(s) of the person(s) the Client lives with;
- Religious beliefs;
- Name of next of kin;
- Name of emergency contact;
- Details of Lasting Power of Attorney;
- Name(s) of people who are involved in the Client's care;
- Name of the Client's General Practitioner;
- Name of the Client's Physiotherapist;
- Name of the Client's Speech and Language Therapist;
- Names of other contacts relevant to the Client's health and wellbeing;
- Details of recent hospitalisation and record of any disabilities;
- Record of any infectious diseases;
- Reason(s) for care and support;
- Details of all medication taken;
- Mobility;
- Details relating to assistance needed with money and finances;
- Details relating to all aspects of daily living where the Client may need support;
- Spirituality and Religious beliefs;
- Assistance with general healthcare needs;
- Things that are important in relation to the Client's life;
- The Client's worries;
- The Client's goals in life;
- The Client's likes and dislikes;
- Details relating to the Client's emotional health;
- Details of any allergies/phobias;
- Aspects of daily living the Client prefers to do him/herself;
- Aims to improving independence
- Communication issues;
- Risks to the Client's health and safety.

Clients may refer to the Company's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

Data protection principles

All personal data obtained and held by the Company will:

- be processed fairly, lawfully and in a transparent manner;
- be collected for specific, explicit, and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes of processing;
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay;
- not be kept for longer than is necessary for its given purpose;
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures;
- comply with the relevant GDPR procedures for international transferring of personal data, where appropriate and relevant.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed;
- the right of access;
- the right for any inaccuracies to be corrected (rectification);
- the right to have information deleted (erasure);
- the right to restrict the processing of the data;
- the right to portability;
- the right to object to the inclusion of any information;
- the right to regulate any automated decision-making and profiling of personal data.

The Company has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it appoints or employs employees with specific responsibilities for:

    a) the processing and controlling of data;
    b) the comprehensive reviewing and auditing of its data protection systems and procedures;
    c) overviewing the effectiveness and integrity of all the data that must be protected.

There are clear lines of responsibility and accountability for these different roles.

- it provides information to its Clients on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way;
- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with;
- it carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the Company;
- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The Company understands that consent must be freely given, specific, informed and unambiguous. The Company will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time;
- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences;

Access to data

Relevant individuals have a right to be informed whether the Company processes personal data relating to them and to access the data that the Company holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- a form on which to make a subject access request is available from a member of the Management Team;
- the Company will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the Client making the request;
- the Company will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform the Company immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The Company will take immediate steps to rectify the information. For further information on making a subject access request, Clients may refer to the Company's subject access request policy, available from a member of the Management Team.

Data disclosures

The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- individuals' health data - to comply with health and safety or other health obligations towards the Client;

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data security

The Company adopts procedures designed to maintain the security of data when it is stored and transported. More information can be found in the data transfer security policy, available from a member of the Management Team.

In addition, employees of the Company must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them;
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people;
- check regularly on the accuracy of data being entered into computers;
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them;
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to Clients should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by a member of the Management Team. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary;
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted;
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

International data transfers

[Select from the paragraphs below and delete as appropriate]

The Company does not transfer personal data to any recipients outside of the EEA.

[OR]

The Company may be required to transfer personal data to a country/countries outside of the EEA. This is because [insert reasons]. Where this occurs, the following safeguards are adopted [insert details e.g. binding corporate rules/standard data protection clauses/compliance with an approved code of practice etc]

Breach notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the Company becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual. If the breach is sufficient to warrant notification to the public, the Company will do so without undue delay.

Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach. The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under the GDPR. All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

Records

The Company keeps records of its processing activities including the purpose for the processing and retention periods. These records will be kept up to date so that they reflect current processing activities.

[Select from the paragraphs below and delete as appropriate]

Data Protection Officer

The Company's Data Protection Officer is [insert name]. [Delete as appropriate – He/She] can be contacted at [insert details].

[OR]

Data protection compliance

[Insert name] is the Company's appointed compliance officer in respect of its data protection activities. [Delete as appropriate – He/She] can be contacted at [insert details].

KLOE References for this Policy	Regulations directly linked to this Policy	Regulation(s) relevant to this Policy
Safe **Well-Led**	**Regulation 9: Person-centred care** **Regulation 10: Dignity and respect** **Regulation 11: Need for consent**	