PRIVACY NOTICE

As your service provider, Lauriem Complete Care Ltd needs to keep and process information about you for service provision purposes. The information we hold and process will be used for our management, administration, service delivery and your Health and well being use only. We will keep and use information to enable us to deliver and manage a safe and effective service, lawfully and appropriately, whilst we are delivering a service to you, at the time when your service ends and after you have left. This includes using information to enable us to comply with any legal requirements, pursue the legitimate interests of the Company and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision. We will do all we can to respect your right to privacy and the protection of your personal information. Below is a breakdown of what we do with your information in order to run the business and protect your data.

1. What client data we hold

Lauriem Complete Care Ltd will hold personal data about you during and after your service, this data will be held in your client file and on our Rostering system. Much of the information we hold will have been provided by you, but some may come from other external sources, such as Social Service, NHS, District nurses and / or other health care professionals. The data we will hold will include:

- Name, address, date of birth,
- Next of kin
- Ethnic Origin
- Terms & Conditions of Service
- Health Conditions
- Prescription Medication
- Meeting notes
- Safeguarding
- Risk assessment / care plan

We process and share special categories of information relating to your health and wellbeing, this data is requested as part of our contractual obligations with KCC and the NHS. We will always obtain your explicit consent to those activities unless this is not required by law or the information is required to protect your health in an emergency. Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

You will, of course, inevitably be referred to in many company documents and records that are produced by our staff in the course of carrying out their duties and the business of the company.

2. What client data we process, share and why

Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so, to fulfil any organisation contracts (such as Kent County Council) or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to other organisations. This means, for example that we will pass some information to the Care Quality Commission (CQC), GP's and other health care professionals. We will also give details to the police where we are legally required to do so, i.e. in emergencies and where crime detection or prevention can be aided by the release of the data.

Your data will be used:

- Kent County Council contract agreements
- Care Quality Commission (CQC) requirements
- Health and Wellbeing
- Service Provision

The sharing of your data as specified above is necessary for the purposes of legitimate interests pursued by the organisation or third party and / or we are under a contractual obligation to provide this information. All data will be held securely and in accordance with the Data Protection Act 1998 (DPA) and the General Data Protection Regulations (GDPR). All data that we process is at its minimal and relevant. No excessive or unnecessary data is allowed to be processed without your consent or other lawful reason.

3. Who will have access to my data & how will it be stored

Your basic personal details are accessible to office staff via our rostering system (name, address, email, next of kin and telephone number), all other data including sensitive data, for example- details relating to any health & disability documentation is only accessible by Human Resources and the Senior Management Team. All personal data is held in your client file, your file is kept in a locked filing cabinet in a secured room that is only accessible to Managers.

All electronic information held about you has restricted access and / or is password protected, again this is only accessible by Lauriem Complete Cares' staff. Once clients have left our service their basic details will remain on our IT system for reference purposes. All other information will be stored securely onsite or sent to our offsite secure storage holding facility in the UK and stored for the specified period as laid out in the table below (Appendix 1). The Company follows the retention periods recommended by the Information Commissioners Office. You should therefore treat the following as guidelines for retention times in the absence of a specific business case supporting a longer period.

Data	Duration
Purchase order	3 years following cessation of service
Risk Assessment / Care Plan	3 years following cessation of service
Safeguarding	3 years following cessation of service
Complaints	3 years following cessation of service
NOK Details	3 years following cessation of service
Health Care Professionals contact details	3 years following cessation of service
Health Conditions	3 years following cessation of service
Visit Record Books / MAR Charts	3 years following cessation of service

Appendix 1.

Once that period has passed, the information will be confidentially and securely disposed of. Access to this facility is by Senior Management only. No personal data will be transferred outside the EEA without your written consent. We will not release data to anyone who is unauthorised. If you wish for your data to be released in such circumstances you must give consent to this. This means that we will not release data to banks, friends, relatives, etc. without your agreement. If you wish us to provide information to someone such as a bank you should contact us to give

consent, either directly or through a third party requesting the data, or you should ensure that you pass the third-party request to us yourself.

4. Who to contact should you need to amend / update your data

If you need to update your personal data please contact the area coordinator with your new details. It is your responsibility to inform us if data we hold about you requires updating. You must notify us immediately if your personal data changes, for example, your address. We will however, provide periodic opportunities for you to update your data through staff meetings and via the annual update your personal details form.

5. How can you access your data

Under the General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) you have a number of rights with regard to your personal data. You have the right to request from us access to and rectification or erasure of your personal data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability. If you have provided consent for the processing of your data you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn. All requests should be made in writing to the Registered Manager

6. What can you do if you have any objections

You are entitled to raise an objection where the processing of data we hold about you is likely to cause damage or distress (subject to provisions contained in the Data Protection Act 1998) or if you have any objections to the data processing procedures we have in place, all objections will be logged showing the appropriate action that was taken in response to the objection, for example. such as the deletion of data. All requests should be made in writing to the Registered Manager outlining your objections.

7. Security and Responsibilities

We shall both, at all times comply with the General Data Protection Regulations with regard to the provision of your service and thereafter, within this agreement and shall under no circumstances make the other party in breach of these laws, rules or regulations.

a) No personal information regarding a Service User or employee shall be carried in person without written prior authorisation from the named person and Senior Management.
b) All electronic devices holding personal data, for example laptops, tablets and Lauriem's mobile phone App are to be locked at all times when not in use.
c) The sharing of information is prohibited without written consent.
d) No personal data is to be moved from its original source without specific consent from a member of the Senior Management Team (i.e. visit record books, SU files, MAR)
e) No Service Users, their families or employee's personal details including telephone numbers are to be held on any personal electrical device (i.e. mobile phone, tablet, laptops) without their consent and Senior Managements authorisation.
f) No written personal details about a Service User, their family or an employee is to be held i.e. telephone numbers, addresses, key safes, email addresses, without their consent and Senior Managements authorisation.

All new staff are encouraged to read the policies on data protection and on confidentiality as part of their induction process. Existing staff will be offered training to National Training Organisation standards covering basic information about confidentiality, data protection and access to records. Training in the correct method for entering information in service users' records is given to all care staff.

Data Access control systems are in place to reduce the risk of unauthorised access to your data, i.e. strong and secure passwords, restricted access, all data locked away, Clean Desk Policy. A Clean Desk Policy is in operation, this will help reduce the risk of unauthorised access to sensitive and confidential documents and data. Our IT system is maintained by a third party (BCTec and Anthony Lodge) whom have access to our IT system to provide system updates, ensure daily back-ups are completed and ensuring we have adequate security (e.g. firewall, anti-spam, virus protection, etc.).

We regularly review and update our data protection policy, procedures and notices to ensure they are accurate, relevant and fit for purpose.

8. Who to report a data breach to, and when to report it

If you feel there has been any data breach of any kind we would urge you to contact the Registered Manager to report your concerns immediately. Full details of the suspected breach will be taken and investigated fully. All serious breaches in data will be escalated to the Managing Director and the Information Commissioners Office will be notified where applicable. Appropriate action will then be taken with regards to the consequences of the breach.

You also have the right to lodge a complaint to the Information Commissioners' Office if you believe that we have not complied with the requirements of the GDPR or DPA 18 with regard to your personal data.

9. The consequences of a data breach

Any breaches to data protection are treated very seriously, all breaches will be thoroughly investigated and appropriate disciplinary action taken where necessary. A review of our policies and processes may ensue to ensure further occurrences do not arise.

10. Reviewing the data we hold & process

We will regularly review and update our data protection policy, procedures and notices to ensure they are accurate, relevant and fit for purpose. All staff will be offered training to National Training Organisation standards covering basic information about confidentiality, data protection and access to records.