Data Protection Policy

Organisation name : Terravita WTP

Registration reference: C1601766

Date registered : 15/11/2024

Responsibility for controlling and processing assigned to Anneka Schofield (Manager).

Customer enquiry contact details: anneka.schofield@terravitawtp.co.uk

Email address: anneka.schofield@terravitawtp.co.uk

Under the Data Protection Act 1998 (DPA) and in line with GDPR Terravita WTP will:

- use personal information fairly and lawfully;
- collect only the information necessary for a specific purpose(s);
- ensure it is relevant, accurate and up to date;
- only hold as much as we need, and only for as long as we need it;
- allow the subject of the information to see it on request; and allow them to request to withdraw their information.
- keep it secure.

Nature of work description:

Reasons/purposes for processing information: We process personal information to enable us to provide:

- Training for young people
- therapeutic sessions
- Supervision,
- to monitor our services,
- to promote our services,
- to maintain our own accounts and records,
- to support and manage our employees/workers/students.

When we hold data we will inform the individual of the data we hold, how we store it, how long we keep it for and who it is shared with. They can request to see that data and we will provide that within 30 days. They can request for the data to be corrected, erased or the processing restricted.

Type/classes of information processed:

We process information relevant to the above reasons/purposes. This may include:

• personal details

• family details

• financial details of workers for the purpose of payment

• training details

• education and employment details

We also process sensitive classes of information that may include:

• physical or mental health details

• racial or ethnic origin

• professional body membership

• DBS details

• Insurance details

• Personal identification documents

Who the information is processed about

We process personal information about:

• Customers (schools, organisations, individuals) – email addresses and contact numbers, names of and roles of staff/individuals

• Clients (adults and children) – personal details

• Students – contact and relevant personal details

• Workers - contact details, relevant personal details, and finance for payment

• suppliers – contact details and finance for payment

How the information is stored

Where ever possible data is stored electronically. Laptops are password protected and have Protection e.g. Norton.

Documents containing personal information are password protected when sharing (see below).

Where paper records are kept these are stored in a private building, in a locked filing cabinet.

Data will be kept until it is no longer needed for the reasons or purposes listed above, or in certain cases in line with legal requirements (e.g. Looked after or Adopted Children).

As stated above, individuals can enquire as to how long their data will be kept for. Who the information may be shared with We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA) and with GDPR.

Types of organisations

We may need to share some of the personal information we process with for one or more reasons. Where necessary or required we share information with:

• our workers

• other involved professionals

• professional clinical supervisors

• educators and examining bodies

• current, past or prospective employers

• family, associates and representatives of the person whose personal data we are processing

- financial organisations – when paying workers
- suppliers and service providers
- persons making an enquiry or complaint

When information is shared it is anonymised (where appropriate) and sent by email with a password protection.

Undertaking research

Personal information is also processed in order to undertake research. For this reason the information processed may include name, contact details, family details, lifestyle and social circumstances. The sensitive types of information may include physical or mental health details, racial or ethnic origin. When used for research the individual will not be identifiable from the data. Data is anonymised. Where necessary or required this information may be shared with customers and clients, workers, service providers, survey and research organisations.

Consulting and advisory services Information is processed for consultancy and advisory services that are offered. For this reason the information processed may include name, contact details, family details, lifestyle and social circumstances. The sensitive types of information may include physical or mental health details, racial or ethnic origin. This information may be about customers and clients. Where appropriate this information is shared with the data subject themselves, family members, business associates and other professional advisers and service providers.

Marketing Contact information of schools organisations and individuals is held in order to promote our services. All mail sent have a clear 'Unsubscribe' option which is an monitored email address for this purpose. The manager then removes their contact details. This is done before the next email round.

Where an email is a personal one the individual has been a previous client and has opted in to being on our mailing list.

Worker Training

All workers delivering therapeutic intervention work for Terravita WTP are required to be registered with the ICO and to follow the legal requirements.

We provide workers with guidance as to how to comply with legal requirements.

When there are changes to the legal requirements Terravita WTP will ensure all workers are aware and sign post them to any relevant training.

Incident Management

A Personal Data Incident (also referred to as a Data Breach) is any situation where there has been an accidental or unlawful destruction, loss of access or availability, alteration, unauthorised disclosure of, or access to, personal data. It should be noted that if personal data becomes incorrectly exposed to others, but the data is not used by others, then this still constitutes a Personal Data Incident.

Below are some more common examples of data incidents:

• access by an unauthorised third party;

• deliberate or accidental action (or inaction) by a data controller or processor which causes the above effects;

• sending personal data to an incorrect recipient

• revealing other recipients by failing to use the BCC field when sending mass communications via email;

• publishing personal data in the public domain (when we do not have consent to do so);

• communicating with individuals who have not consented to receiving communication from Wyldewood farm;

• computing/mobile devices containing unencrypted personal data being lost or stolen
• alteration of personal data without permission; and o loss of availability of personal data.

Incident Management and Reporting

Should there be an incident regarding a data breach the relevant parties are to initially report the details to the company manager.

This should be done immediately and followed up by an email.

- All emails should identify the subject matter as a '**data incident'** in the email title.
- all emails should be marked as confidential.
- all emails should be marked as high priority.

A record will be made of the relevant details and advice will be sort from the ICO as to the required form of action. This needs to be reported to ICO within 72 hours of the breach. Therefore it is essential that workers report any data breach incidences to farm manager immediately, even if off-duty.

Post incident the relevant parties will meet with the manager to decide what needs to be put in place to ensure that the situation is not repeated. A time scale will be specified for the changes to be implemented.

Complaints

Complaints Handling Should someone have a complaint about Data protection initially they will be directed to the Terravita WTP Manager. The complaint will be acknowledged within 5 working days and a response provided following an investigation within 1 month providing sufficient details are included to investigate. A record will be made of the relevant details and attempts will be made to resolve the situation. If the complainant is still dissatisfied, then the requester will be informed that they can register their complaint with the ICO. In this case advice will be sought from the ICO.

Post incident or complaint, the Directors will meet to decide what needs to be put in place to ensure that the situation is not repeated. A time scale will be specified for the changes to be implemented.

Review

This policy and the Data protection procedures will be formally reviewed every year and changes communicated to all relevant parties.

Date for review: June 2027.

Ongoing reviews and changes will also take place in response to information and situations

For more information, visit Information Commissioner's Office (ICO).