

GDPR version 2 16/04/2018

COMFORT HOME CARE

 GENERAL DATA PROTECTION REGULATIONS 2016/ 679- STATEMENT OF COMPLIANCE

Set out below are details of the way in which Comfort Home Care receives, stores, secures and destroys data.

Data Receipt

Data relating to the Payroll, Human Resource Service Users are received in the following formats

In Person – Documents handed physically to senior staff at the premises.

By Post – Post is received in a locked post box at the front of the premises.

Electronically – The information arrives by email to one of the 3 e-mail addresses used by the company.

Data Storage/ Data Security

Hard copy data

Data stored in hard copy is kept in the office, in locked cupboards. Archive data is kept in the office, in locked cupboards. The office door is kept locked when not attended. Keys to locked cupboards are held by senior management only. Keys to the office door are held by senior management only (with the exception of the Manager of Sunningmead Community Centre under their own data protection and confidentially policies – available on request). All staff are required to accept and sign confidentially agreements, and then hard copy data which could be classed as sensitive is only supplied on a need to know basis.

Electronic Data

Electronic data is divided into 2 types, email data and locally stored data.

 E mail data – Comfort Home Care uses Outlook on password protected computers for its main email requirements. The company also uses web-based NHS email accounts and an Egress Switch account for the transfer and attachment of sensitive data, for example, Care Plans.

Payroll data and Client data are transferred to GDPR complaint companies and authorities via password protected documents. We do not transfer any data ourselves outside the EU. Companies used for data storage by our payroll company may transfer data outside of the EU - but such transfers are made in full compliance with all EU regulations. We are satisfied, based on our knowledge at the time of producing this statement, that our pay roll company and all local authorities that we deal with have taken all necessary steps to comply with GDPR. Further information is available upon request.

The company computers holding email data are all secured with passwords inside our office premises, which is kept locked when not attended.

 Locally stored electronic data - All locally stored electronic data, other than selected e mail data, is held on local computers which are secured with passwords. Backups of the data are made daily to a separate storage device which is password secured and kept in a locked cupboard in the office.

Data is never accessed remotely. Computers connected to the internet have their operating systems updated when prompted, and all company computers are protected by up to date anti-virus software and scheduled virus scans.

Disposal/ Removal of Data

Hard copy data

All hard copy documents relating to clients are staff are kept for 6 years.

Hard copy data which is deemed to have expired in this is collected by a data destruction company in sealed bags provided by the company for this purpose. A certificate of destruction is provided by the company for each collection.

The office has a cross cut shredder which is used to destroy unwanted paperwork which does not fall into the categories above.

Electronic data

Unwanted electronic data is deleted from the company’s computer as required by the company.

Requests for data destruction/ deletion from the Companies Clients

Requests from the company’s clients or staff members for data whether in hard copy or electronic form to be destroyed or deleted will be actioned, subject to conditions, within 14 days. The request must be given either in writing or by mail from the client or staff member, or an authorised representative of the client or staff member. The request will be acknowledged in writing in the same manner and confirmation given of the action taken after it’s completion within a further 7 days.