

1. Data protection policy

- 1.1 We take our responsibility to protect personal data very seriously. This policy sets out how we handle your personal data. If you're an employee, you'll be given access to a data protection policy relating to you and your employment - this policy doesn't relate to you.
- 1.2 We have appointed a Data Protection Officer, Joe Rice, who is accountable for ensuring your personal data is processed lawfully. If you have any questions about this policy or the processing of personal data they would be delighted to help you to answer them.

What personal data do we hold?

If we hold any of your personal data, you should have already received a privacy notice which lets you know what personal data we may hold on you. If you would like another copy, please email us at: info@countrycourtcare.com.

Protecting personal data

- 1.3 There are eight principles that we follow when processing your personal data. They are that it must be:
- (a) Processed fairly, lawfully and transparently;
 - (b) Relevant and not excessive;
 - (c) Processed for limited purposes and in an appropriate way;
 - (d) Accurate;
 - (e) Not kept longer than necessary;
 - (f) Processed in accordance with the laws dealing with personal data;
 - (g) Kept secure;
 - (h) Not transferred to people or organisations in other countries without adequate protection.

Here's a bit more detail....

- 1.4 We process personal data fairly and lawfully. Grounds for processing personal data include; with consent, to comply with a legal obligation, in the data subject's vital interests, in the performance of a contract with the data subject or in our legitimate interests. If the personal data is sensitive, additional conditions will be met.
- 1.5 Where we don't have an alternative lawful basis to process your personal data we'll ask you for your consent to do so. In particular, we will only send you marketing emails or make contact about marketing initiatives where you have agreed to us doing so.

- 1.6 We will always be transparent about how we're using your personal data. We'll provide you with information about who controls your data, how and why it will be used, how it's protected and how long it's retained for within a privacy notice (which will usually be found on our website).
- 1.7 We might contact you:
- (a) to ensure that the information that we hold remains accurate;
 - (b) to invite you to participate in surveys;
 - (c) to update you on material changes to policies and practices;
 - (d) in relation to any correspondence that we receive from you;
 - (e) for marketing purposes; or
 - (f) in respect of any complaint we receive.
- 1.8 If you know that the personal data that we hold is inaccurate please notify us as soon as possible so that we can make the necessary changes, where appropriate.
- 1.9 Wherever possible, personal data will be anonymised, encrypted, password protected or subject to any other appropriate security measures so that it is not accessible to others.
- 1.10 Personal data will be deleted in accordance with 'our policy for retaining your personal data'. Please ask us for a copy.
- 1.11 If you become aware that personal data has been lost, stolen or transferred to someone inappropriately or without authorisation, please inform our Data Protection Officer immediately.

Requests to see your personal data

- 1.12 If you want us to show you personal data that we hold on you then you need to make a request in writing to our Data Protection Officer. We might ask you for more details about the request or give you a template letter to help with your request. Where the request isn't made in person we will always ask for two forms of identity to confirm that it is you making the request.
- 1.13 We'll always try and acknowledge your request when we receive it. We've got between 30 days and three months to respond in full to your request.
- 1.14 We may ask you to contribute towards the administration fee in processing your request.

Your rights to deletion, freezing data processing and corrections

- 1.15 You can ask us to delete your personal data where:
- (a) Processing it is no longer necessary bearing in mind the reason it was collected;

- (b) It is being processed unlawfully;
- (c) You object to us processing your personal data (unless we have an over-riding legitimate interest for continuing to process it in which case we may continue to do so).

1.16 Where information we hold on you is inaccurate or incomplete you can ask us rectify the data.

1.17 You can ask us to stop processing your data where:

- (a) Processing is unlawful;
- (b) You say that the information that we hold is inaccurate;
- (c) You don't consider we have a 'legitimate interest' for processing the data (unless we have an over-riding legitimate interest for continuing to process it in which case we will continue to do so).

If we think that you're abusing these rights and making unfounded or excessive requests we may refuse your request or may charge a reasonable administration fee for processing the request.

Training and audit

1.18 Our employees have undergone training to enable them to comply with this policy.

1.19 We test our systems and processes to ensure we meet with our obligations under this policy.

Automated processing

1.20 Generally, automated decision making is prohibited where the decision has a significant or legal effect on an individual. The exceptions to this are where:

- (a) The data subject has explicitly consented;
- (b) The automated processing is automated by law; or
- (c) The automated processing is necessary for performing or entering into a contract.

1.21 If a decision is to be based on automated processing, we will inform you of this and let you know of your right to object. We'll give you information on the logic involved in the decision making and give you the right to request human intervention, or to challenge the decision.

1.22 Before any automated processing is carried out, an impact assessment must be carried out.

Sharing personal data

1.23 Generally, we don't share your personal data with third parties. We'll only do so where:



Our family, caring for yours

- (a) It is required by law (for example, to government bodies);
- (b) They need to know the information in order to fulfil their contract with us (but provided they will not use your information for their own purposes);
- (c) Internally where we need to do so to comply with our obligations to you;
- (d) You've been informed and your consent has been obtained (where we have identified it is needed);
- (e) The third party has adequate security measures in place;
- (f) The transfer complies with any applicable restrictions on cross-border transfers;
- (g) A fully executed written contract which contains GDPR compliant clauses has been obtained.