PRIVACY POLICY

The Gingerbread Clinic is committed to protecting and respecting your privacy.

This policy (and any other documents referred to on it) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it. By visiting you are accepting and consenting to the practices described in this policy.

For the purposes of the Data Protection Act 1998 (the **Act**), the data controller is Claire Sanderson (or whichever practitioner treats you). The Gingerbread Clinic. 7a East Street, St Ives, Cambs, PE27 5PB.

The rules on processing of personal data are set out in the General Data Protection Regulation (the "GDPR").

1. Definitions

Data controller - A controller determines the purposes and means of processing personal data.
Data processor - A processor is responsible for processing personal data on behalf of a controller.
Data subject – Natural person

Categories of data: Personal data and special categories of personal data
Personal data - The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier (as explained in Article 6 of GDPR). For example, name, passport number, home address or private email address. Online identifiers include IP addresses and cookies.

Special categories personal data - The GDPR refers to sensitive personal data as 'special categories of personal data' (as explained in Article 9 of GDPR). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Other examples include racial and ethnic origin, sexual orientation, health data, trade union membership, political opinions, religious or philosophical beliefs.

Processing - means 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.

Third party - means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

2. Who are we?

Claire Sanderson and staff at the clinic are the data controller for any data on PPS. This means we decide how your personal data is processed and for what purposes. As we provide a service to the patients, they are their own data processor. Our contact details are: Claire Sanderson. The Gingerbread Clinic, 7a East Street, St Ives, Cambs, PE27 5PB For all data matters contact Claire on 01480 300029, 01480 469414, 07729 420663, email claire@gingerbreadclinic.co.uk

Philip Kingsland, Charlotte Begg, Victoria Ayton are also data controllers for their own patients and are responsible for their own patients' data.

PPS is the data processor for us for as long as the client data is on PPS.

Claire and the practitioners are the data processor for any data Not on PPS but held on any other system including paper.

3. The purpose(s) of processing your personal data

We use your personal data for the following purposes:

- Health care needs.
- Employee information.

- With reference to the categories of personal data described in the definitions section, we process the following categories of your data:

- Personal data. Contact details and health records. Employee details, payroll, contracts, records and sick leave. Practitioner contact details and contracts.

We have obtained your personal data from you.

INFORMATION WE MAY COLLECT FROM YOU

We may collect and process the following data about you:

- **Information you give us.** You may give us information about you by filling in forms or by corresponding with us by phone, e-mail or otherwise. This includes information you provide when you register to see a practitioner. The information you give us may include your name, address, e-mail address and phone number, GP, health records financial information and employment details (employees only).

- **Information we collect about you.** With regard to each of your visits, we may automatically collect further health records from you.

  Information we receive from other sources. We may receive information about you from other healthcare providers.

5. What is our legal basis for processing your personal data? (article 6 of GDPR)

As part of your health records which act as legal documents.

As part of employment records.

We require your personal data as it is a contractual requirement and necessary to treat /employ you

Legal Basis of Processing – What data is being processed and why?

All information processing must be done under a 'lawful basis of processing'. There are six separate lawful bases of processing set out under GDPR Article 6. Each of these are listed and summarised below:

Consent – The individual has provided clear consent to their data being used for the specific purpose it is being used. This is not a 'one-off' event but instead is continual, when information is processed based on consent the individual can withdraw their consent whenever they please and we must comply with this. It is our responsibility to prove that we have obtained consent from the individual and demonstrate that we have complied with the regulations to make this consent valid.

Contract – The processing is required to allow us to fulfil our contractual obligations to the individual or because they have asked us to do something before entering into a contract, such as providing a quote. This does not need to be a formal written contract, provided the exchange meets the requirements of contract law.

Legal Obligation – We need to process the data to comply with a legal obligation that we are subject to. This could include, for example, legal requirements relating to clinical oversight or accounting regulations.

Vital Interests – If we need to process the data to protect an interest vital to the life of any individual then we can rely on this basis of processing.

Public Task – The information processing is required for the completion of a task in the public interest or for the exercise of official duties. This will generally apply to public authorities but may also apply to some organisations that perform these tasks.

Legitimate Interests – If we have a legitimate interest in using the information then we may be able to rely on this basis of processing. This is the most flexible reason for processing but comes with some additional responsibilities to us, the controller, including evaluating if the processing is necessary for the specific interest, if the individual could reasonably expect us to use their data in this way and if it can be achieved by another

means. In order to process data under the legitimate interests basis, we will need to perform a balancing test to ensure that the interests of our organisation in using the data for this purpose are not outweighed by the individual's rights and freedoms.

As a data controller is it our responsibility to identify what personal data we are processing, why we are processing it and what legal basis applies to each processing activity. Any personal information that we process must be done so under one of the reasons above, if we cannot process the data under one of these reasons then we have no legal basis to process the data.

There is additional protection provided to 'special categories of personal data', data that may be particularly sensitive, including information on racial or ethnic origins, data concerning a person's sexual orientation and, importantly here, information on the data subject's health, that prohibits their use in most cases. In order to process special data we must identify a condition of processing under Article 9 in addition to the legal basis of processing of the data. In the case of clinics providing healthcare services, this will be processing necessary for the provision of health or social care.

Information we collect about you. We will use this information:

- as part of patient/practitioner/employee records.
- As part of your healthcare records.

- **Information we receive from other sources.** We may combine this information with information you give to us and information we collect about you. We may us this information and the combined information for the purposes set out above (depending on the types of information we receive).

DISCLOSURE OF YOUR INFORMATION

We may share your information with selected third parties including:

- Those that work as part of the clinic, such as practitioners, virtual receptionist, PPS, KTS and those that help in the everyday running of the clinic, accountant, payroll etc
- With your GP or other healthcare providers with your permission.
- Occasional audits of clinical outcomes for insurers or research purposes.

We may disclose your personal information to third parties:

- If we sell or buy any business or assets, we may disclose your personal data to the prospective seller or buyer of such business or assets.
- If the Gingerbread Clinic or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets.

- If we are under a duty to disclose or share your personal data to comply with any legal obligation, or in order to enforce or apply our terms of use and other agreements; or to protect the rights, property, or safety of The Gingerbread Clinic, our customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.]

WHERE WE STORE YOUR PERSONAL DATA

All information you provide to us is stored on secure servers.

We have encryption on all documents that are backed up on boxsync.

Data is password protected.

All third parties involved in the running of the clinic including virtual receptionist, payroll, accountant have provided GDPR compliance statements.

All practitioners have access to data on devices that are password protected and have provided GDPR compliance statements.

Any paper records are kept in locked filing cabinets.

All credit card slips are kept in locked filing cabinets. We are PCI DSS compliant.

Receptionists have been trained in GDPR awareness and have signed GDPR compliance statements.

All reasonable precautions to protection of data has been taken.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

YOUR RIGHTS

You have the right to ask us to delete your data.

You have the right to ask us to share your information.

6. Your rights and your personal data

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data:

- The right to request a copy of the personal data which we hold about you;

- The right to request that we correct any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary to retain such data;
- THE RIGHT TO WITHDRAW YOUR CONSENT TO THE PROCESSING AT ANY TIME, WHERE CONSENT WAS YOUR LAWFUL BASIS FOR PROCESSING THE DATA;
- The right to request that we provide you with your personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable i.e. where the processing is based on consent or is necessary for the performance of a contract with the data subject and where the data controller processes the data by automated means);
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable i.e. where processing is based on legitimate interests (or the performance of a task in the public interest/exercise of official authority); direct marketing and processing for the purposes of scientific/historical research and statistics).

7. Transfer of Data Abroad

WE DO NOT TRANSFER PERSONAL DATA OUTSIDE THE EEA.

8. Sharing your personal data

Your personal data will be treated as strictly confidential, and will be shared only with other healthcare providers such as your GP, consultant or healthcare company with your permission.

9. Automated Decision Making

WE DO NOT USE ANY FORM OF AUTOMATED DECISION MAKING IN OUR BUSINESS.

How long do we keep your personal data?

We keep your personal data for no longer than reasonably necessary for a period of 8 years or in the case of a child, 8 years after their 18th birthday, to be able to provide evidence of healthcare records. Employee and practitioner records are kept for 7 years as part of employment record.

ACCESS TO INFORMATION

The Act gives you the right to access information held about you. Your right of access can be exercised in accordance with the Act.

CHANGES TO OUR PRIVACY POLICY

Any changes we may make to our privacy policy in the future will be posted on this page and, where appropriate, notified to you by e-mail. Please check back frequently to see any updates or changes to our privacy policy.

CONTACT AND COMPLAINTS

Questions, comments, and requests regarding this privacy policy are welcomed and should be addressed to claire@gingerbreadclinic.co.uk

To exercise all relevant rights, queries, or complaints please in the first instance contact on 01480 300029/ 07729 420663. Claire Sanderson.
If this does not resolve your complaint to your satisfaction, you have the right to lodge a complaint with the Information Commissioners Office on 03031231113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, England.