Information Governance & GDPR Policy

Light Touch Clinic

(CYM Limited *trading as* **Light Touch Clinic**)

Policy details

Policy Area: Management Policies	
Document Version	**2.0**
Ratified Date:	**September 2025**
Document Manager	**Selma van den Bosch**
Updated Date:	**September 2025**
Review Date	September 2027

Contents

Introduction

This Information Governance Policy complies with the General Data Protection Regulation (GDPR), Data Protection Act and the Privacy and Electronic Communications Regulations. It explains how Light Touch Clinic handles the Personal Data of patients, employees, and suppliers. This policy is relevant to all personal Data that is processed regardless of the way it is stored. The policy also relates to data of past or present employees, workers, clients or supplier contacts, website users or any other Data Subject.

This policy applies to all staff.

TO ALL STAFF - You must read, understand and comply with the policy when processing personal data. Staff are asked to attend training on its requirements.

This policy sets out what Light Touch Clinic expects from our staff, so that the company is compliant with applicable law. Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

Scope

By correctly and lawfully processing personal data we will preserve confidence in our clients and suppliers. Protecting the confidentiality and integrity of personal data is an important responsibility that we take seriously at all times. The Manager is responsible for ensuring all staff complies with this policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

Personal Data Protection Principles

Light Touch Clinic complies with the principles relating to processing personal data. The principles set out in the GDPR require Personal Data to be:

- Managed lawfully, fairly and in a transparent way (Lawfulness, Fairness and Transparency).
- Collected only for particular, explicit, and lawful purposes (Purpose Limitation).
- Sufficient, applicable, and limited to what is necessary in relation to the reason for which it is processed (Data Minimisation).
- Correct and where necessary and kept up to date (Accuracy).
- Not kept in a form, which allows identification of individuals for longer than is necessary for the purposes for which the data is processed (Storage Limitation).
- Managed in a way that ensures its security and always protects it against unauthorised or unlawful processing and against accidental loss, destruction, or damage (Security, Integrity and Confidentiality).
- Not transferred to another country without suitable safeguards being in place (Transfer Limitation).

- Made accessible to the individual whom the data belongs to, so that they can exercise certain rights in relation to their personal data (Data Subject's Rights and Requests).
- Light Touch Clinic is accountable for and must be able to show compliance with the data protection principles listed above (Accountability).

Lawfulness, Fairness, Transparency

Personal data must always be processed in a lawful, fair, and transparent way.

Personal data should only be collected or shared for specified purposes.

The GDPR restricts actions concerning personal data. These limitations are not intended to prevent data management but to ensure that we process personal data fairly and without adversely affecting the individual.

The GDPR allows processing for specific purposes, some of which are set out below:

a. The individual whom the data belongs to has given his or her consent;
b. The processing is necessary for the performance of a contract with the individual;
c. To meet our legal compliance obligations; and
d. To protect the individuals fundamental interests

Consent Limit

Personal data must only be processed on the basis of one or more of the lawful basis set out in the GDPR, which includes consent. Consent for processing personal data from the individual whom the data belongs to must be indicated clearly in the agreement. Where consent is given in a document, which deals with other matters, the consent element of the documentation must be kept separate from those other matters. Individuals must be easily able to withdraw consent to processing, at any time and withdrawal must be immediately honoured. If personal data is used for a different and incompatible purpose, which was not disclosed when the individual first consented; consent may need to be refreshed.

Transparency (Notifying Data Subjects)

The GDPR requires the person obtaining consent to give detailed, specific information to data subjects depending on whether the information was collected directly from them or from elsewhere. Such information must be provided through suitable privacy notices or fair processing notices which must be succinct, transparent, comprehensible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner unsuited with those purposes.

Personal data cannot be used for new, different, or incompatible purposes from that disclosed when it was first obtained, unless you have informed the person you have taken the data from. They must be informed of the new purposes and be consented where necessary.

Data Minimisation

Personal data must be sufficient, relevant, and limited to what is necessary in relation to the purposes for which it is collected. Personal data must be processed in line with regulation data and cannot be used for any reason unrelated to what it was ascertained for.

We ensure when personal data is no longer needed for specified purposes, it is deleted or anonymised.

Accuracy

Personal Data must be accurate and kept up to date where necessary.

We ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it.

At the point of collection data must be checked to ensure it is correct.

We will take reasonable steps to destroy or amend inaccurate or out-of-date personal data.

Storage Limitation

Identifiable personal data must not be kept for longer than is necessary or for the purposes it was collected.

Security Integrity and Confidentiality

Personal data must be secured by appropriate technical measures against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

Light Touch Clinic will develop, implement, and maintain safeguards appropriate to maintain data and identify risks to data management (including use of encryption). We will regularly evaluate those safeguards to ensure the security of our processing is safe.

Light Touch Clinic maintains data security by protecting the confidentiality, integrity, and availability of the personal data, defined as follows:

- Confidentiality means that only authorised people and those people who have a need to know reason for accessing the information have access.
- Integrity means that personal data is correct and suitable for the reason for which it is processed.
- Availability means that authorised users are able to access the personal data when they need it for authorised purposes.
- Staff must follow all procedures that have been put in place to maintain the security of all personal data from the point of collection to the point of destruction.

Reporting a Personal Data Breach

The GDPR requires those who have collected data to notify any personal data breaches to the applicable regulator.

Do not attempt to investigate any potential personal data breach. Always contact the manager immediately and preserve all evidence relating to the potential breach.

Data Subject's Rights and Requests

Clients have rights when it comes to how their personal data is handled. These rights include:

- Withdrawing their consent to processing their information at any time.
- Request information about the person who is processing their information.
- Are able to access their personal data when they need to.
- Prevent the use of their personal data being used for direct marketing purposes.
- Request that their data is deleted when it is no longer required for the purposes it was collected for.
- Restrict the processing of their data in specific circumstances

Accountability

Light Touch Clinic has appropriate technical measures in place to ensure when data is collected it is managed in line with data protection principles.

The person collecting the data is responsible for, and must be able to demonstrate, compliance with the data protection principles.

To make sure that the person collecting the data has the knowledge and understanding of the importance of appropriately managing data, they will work in line with the GDPR Policy, data protection guidelines, take consent, report any data breaches, and maintain a record of training.

Record Keeping

Records are kept in full and data is accurately reflected in the notes.

Consent is taken in accordance with GDPR and is always documented.

Records should include the person's name and contact details of the person who has recorded the data.

Training and Audit

Staff will undergo mandatory training for data management to ensure they are aware of how to comply with data privacy laws. (Bluestream e-learning)

Regular tests of our systems and processes to assess compliance and governance controls will take place. We do this by undertaking spot check of records, to make sure that they have the correct details within them, including consent.

Direct Marketing

At Light Touch Clinic we abide by rules and privacy laws when marketing to our customers including electronic direct marketing (for example, by email, text, or automated calls). The exception is when existing customers have opted out of marketing when first collecting their details. If a customer opts out at any time, their details should be hidden as soon as possible.

Sharing Personal Data

We will not share personal data with third parties unless we have consent from the individual whom the data belongs to and certain safeguards and contractual arrangements have been put in place.

Personal data we hold may be shared with another employee if the recipient is in a job that requires that information.

Changes to This Data Privacy Policy

Light Touch Clinic reserve the right to modify this policy at any time without notice to you so please ensure you regularly obtain the latest copy of this policy. This policy does not supersede any applicable national data privacy laws and regulations.

Definitions

	Description
Data Controller	The person who determines when, why and how to process personal data. They are accountable for establishing practices and policies in line with the GDPR.
Data Subject	An individual about whom we hold personal data about
Data Protection Manager	A person appointed with responsibility for data protection compliance.
General Data Protection Regulation (GDPR)	The General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.
Personal Data	Identifiable information about an individual or information relating to an individual that can be identified (directly or indirectly).
Personal data breach	Any act or omission that compromises the security, confidentiality, integrity or accessibility of Personal Data.
Processing or Process	Any actions that involves using personal data. It may involve acquiring, recording, holding the data, or carrying out any process or set of processes on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it.
Sensitive Personal Data	This is information relating to a variety of personal information such as racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health

References

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Data Protection Act 2018

https://ico.org.uk/for-organisations/data-protection-act-2018/

https://www.rcplondon.ac.uk/projects/outputs/standards-clinical-structure-and-content-patient-records