# GDPR

**Pinner Chiropractic Clinic**
**Data Protection Policy**

**Context and overview**
**Key details**

- Policy prepared by: Rachel Lock
- Policy became operational on: 25/05/2018
- Next review / audit date: 01/05/2021

**Introduction**
Pinner Chiropractic Clinic needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the Clinic has a relationship with or may need to contact.
This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.
**Why this policy exists**
This data protection policy ensures Pinner Chiropractic Clinic:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

**Data protection law**
The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) describes how organisations — including must collect, handle and store personal information.
These rules apply regardless of whether data is stored electronically, on paper or on other materials.
To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.
The Data Protection Act is underpinned by seven important principles. These say that personal data must:
a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the

GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
g) Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

**People, risks and responsibilities**

**Policy scope**

This policy applies to:

- The head office of Pinner Chiropractic
- All staff and volunteers of Pinner Chiropractic Clinic
- All contractors, suppliers and other people working on behalf of Pinner Chiropractic Clinic

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation 2016. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

**Data protection risks**

This policy helps to protect Pinner Chiropractic Clinic from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

**Responsibilities**

Everyone who works for or with [Pinner Chiropractic Clinic] has some responsibility for ensuring data is collected, stored and handled appropriately.
Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.
However, these people have key areas of responsibility:

- The business owner Rachel Lock is ultimately responsible for ensuring that Pinner Chiropractic Clinic meets its legal obligations.
- A Data protection officer has not been appointed on the basis that data processing is small scale, and therefore a DPO is not legally required. These responsibilities will be therefore the requirement of the Data Controller Rachel Lock.:
    - Keeping the staff updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.

- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Pinner Chiropractic Clinic holds about them (also called ‘subject access requests’).

- Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

- Performing regular checks and scans to ensure security hardware and software is functioning properly.

- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.

- Addressing any data protection queries from journalists or media outlets like newspapers.

- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

- Performing a formal data protection audit every 3 years, or if poor data protection practices is noticed by any member of staff and brought to the attention of the controller.

**General staff guidelines**

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally.
- Pinner Chiropractic Clinic will provide training when needed to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, passwords must be used and they should never be shared with anyone who does not require data access.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from the data protection controller if they are unsure about any aspect of data protection.

**Data storage**

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.
These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded or incinerated** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** and only shared with employees that require access for their core work.
- All **letter templates** must be either be **irreversibly anonymised**, or **password protected**.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

**Data use**
Personal data is of no value to Pinner Chiropractic Clinic unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular emails addresses must be confirmed prior to sending, potential mistakes can make this form of communication insecure. You may consider email encryption for particularly sensitive data.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

**Data accuracy**
The law requires Pinner Chiropractic Clinic to take reasonable steps to ensure data is kept accurate and up to date.
The more important it is that the personal data is accurate, the greater the effort Pinner Chiropractic Clinic should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

**Subject access requests**

All individuals who are the subject of personal data held by Pinner Chiropractic Clinic are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.
- Patients have the right to data deletion, the right to be forgotten. However this does not supersede the current GCC requirements. Currently adult patient data is required to be held for 8 years following their last appointment. For patients under 18 years of age the file must be held until 26 years of age and a minimum of 8 years from the last appointment

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made in writing with written and signed consent. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged to view their data., however reasonable charges such as photocopying charges may be levied to make paper or digital copies. This will not exceed £50. The data controller will aim to provide the relevant data within 14 days, and this should not take longer than a month.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

If a data request is denied for any reason this must be provided in writing to the subject together with information on how to make a complaint to the information commissioner.

**Disclosing data for other reasons**

In certain circumstances, GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject, or where there is a risk to life.

Under these circumstances, Pinner Chiropractic Clinic will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

**Providing information**

Pinner Chiropractic Clinic aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used

- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.
This is available on request. A version of this statement is also available on the company's website.