PATIENTS COMMUNITY

PRACTICE AND DISTRICT NURSES

LEG CLUB®

www.legclub.org

The Lindsay Leg Club Foundation
CRN 1111259

The Lindsay Leg Club Foundation Data Protection Policy

Key details

- Policy prepared by:
- Approved by board / management on:
- Policy became operational on:
- Next review date:

Definitions

Charity	The Lindsay Leg Club Foundation
GDPR	General Data Protection Regulation
Responsible Person	Named Trustee responsible for data protection within the Charity
Register of Systems	Register of all systems or contexts in which personal data is processed by the Charity

The Lindsay Leg Club Foundation needs to gather and use certain information about individuals. This can include Leg Club clinical and volunteer teams' suppliers, business contacts, external clinical consultants and anyone else the organisation 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 the Lindsay Leg Club Foundation:

- Complies with data protection law and follows 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 Data Protection Act 2018 describes how the Lindsay Leg Club Foundation must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or in any other format.

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 eight important principles. These say that personal data must be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Policy scope

This policy applies to:

- The Lindsay Leg Club Foundation
- All Board Trustees
- All contractors, suppliers and anyone working on behalf of the Lindsay Leg Club Foundation

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. 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 the Lindsay Leg Club Foundation 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

All Trustees and external clinical consultants of the Lindsay Leg Club Foundation have a responsibility to ensure data is collected, stored and handled appropriately.

Each team (e.g. Leg Clubs) that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the board of directors/Trustees is ultimately responsible for ensuring that the Lindsay Leg Club Foundation meets its legal obligations.

- The [data protection officer], [name], is responsible for:
    - Keeping the board 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 the Lindsay Leg Club Foundation 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.

- The named trustee is responsible for:
    - 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.

General 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**. When access to confidential information is required, employees can request it from their line managers.
- Trustees and external consultants should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- 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.
- The board **should request help** 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 trustee responsible for the data.

When data is **stored as a hard copy,** it should be kept in a secure place where unauthorised people cannot access it.

These guidelines also apply to data that is usually stored electronically but has been printed for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- The board of trustees should make sure paper and printouts are **not left where unauthorised people could see them**.
- **Data printouts should be shredded** 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** that are changed regularly and never shared between volunteers, employees and/or trustees.
- Data **stored on removable media** (such as a USB or CD) should be 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 service**.
- 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 charity's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- 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 the Lindsay Leg Club Foundation unless the organisation can make use of it. However, when personal data is accessed and the risk of loss, corruption or theft increases significantly:

- When working with personal data, the board of trustees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Personal data should **never be transferred outside of the United Kingdom**.

Data accuracy

The law requires the Lindsay Leg Club Foundation 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 the Lindsay Leg Club Foundation should put into ensuring its accuracy.

It is the responsibility of all trustees and external consultants 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** and should not create any unnecessary additional data sets.
- The board should **take every opportunity to ensure data is updated.** For instance, by confirming a person's details when they call.

- The Lindsay Leg Club Foundation will make it **easy for data subjects to update the information that** the Lindsay Leg Club Foundation holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a person 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 the Lindsay Leg Club Foundation are entitled to:

- Ask **what information** the organisation holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- The 'right to be forgotten' (Link to ICO explanation: https://bit.ly/2Xmz5lO)

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

Subject access requests from individuals should be made by email, addressed to the data trustee at [email address]. The data trustee can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The data trustee will aim to provide the relevant data within 14 days.

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

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the named trustee will disclose requested data. However, the data trustee will ensure the request is legitimate, seeking assistance from the board and from the Charity's legal advisers where necessary.

Providing information

The Lindsay Leg Club Foundation 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 organisation 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 organisation's website.]

1. Data protection principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

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."

2. General provisions

a. This policy applies to all personal data processed by the Charity.
b. The Responsible Person shall take responsibility for the Charity's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. The Charity shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the Charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The Charity shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

5. Data minimisation

a. The Charity shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. [Add considerations relevant to the Charity's particular systems]

6. Accuracy

a. The Charity shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.
c. [Add considerations relevant to the Charity's particular systems]

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. The Charity shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Charity shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

Adapted from the Information Commissioners Office: The ICO is the UK's independent body set up to uphold information rights.

END OF POLICY