The Lucy Rose Clinic

INTEGRATIVE HEALTH SOLUTIONS

The Lucy Rose Clinic- SAFEGUARDS (Data Security)

Created by: Meredith Bell- Operations Manager

UPDATED : SEPTEMBER 2023

The Lucy Rose Clinic is committed to preserving the privacy and security of all individual's personal data that we collect and handle. This policy outlines the measures we have in place to safeguard this data.

Data Collection: We collect personal data through various methods. This may include information you provide directly to us when you use our services or indirectly through the use of our website, applications, and online platforms .

Data Use and Disclosure: The data we collect will be used for the purpose it was collected for. We do not disclose any personal data to any third parties unless required by law or with the individual's express consent.

Data Protection: We implement strong security measures to protect personal data from unauthorised access, alteration, disclosure, or destruction. This includes physical, electronic, and procedural safeguards.

Data Access and Correction: Individuals have the right to access and correct their personal data. We encourage individuals to keep us informed of any changes to their personal data to ensure it remains accurate and up-to-date.

Virus protection

In order to prevent the introduction of virus contamination into the software system, the following rules must be observed:

- unauthorised software including public domain software, magazine cover disks/CDs or internet downloads must not be used; and
- all software must be virus checked using standard testing procedures before being used.

Use of computer equipment

In order to control the use of the Employer's computer equipment and reduce the risk of contamination, the following rules will apply:

- the introduction of new software must first of all be checked and authorised by management before general use will be permitted;
- only authorised staff are permitted access to the Employer's computer equipment;
- only software that is used for business applications may be used on the Employer's computer equipment;
- no software may be brought onto or taken from the Employer's premises without prior authorisation;
- unauthorised access to computing facilities will result in disciplinary action up to and including dismissal;
- unauthorised copying and/or removal of computer equipment and/or software will result in disciplinary action up to and including dismissal; and
- computer equipment, including laptops, desktops, tablets and mobile phone may not be removed from company premises without prior written approval.

Internet policy

The purpose of this policy is to provide a framework to ensure that the expectations and rules relating to the use of internet within the Employer are clear.

Authorised staff are encouraged to make use of the internet as part of their professional activities. Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the Employer's name. Where personal views are expressed, a disclaimer stating that this is the case should be clearly added to all correspondence.

The availability and variety of information on the internet means that it can be used to obtain material reasonably considered to be offensive. The use of the internet to access and/or distribute any kind of offensive material, or material that is not work-related, leaves an individual liable to disciplinary action up to and including dismissal.

The Employer will not tolerate the use of the internet at work for unofficial or inappropriate purposes, including:

- accessing websites which put the Employer at risk of viruses, compromising copyright or intellectual property rights;
- using social media in breach of the Employer's social media policy;
- connecting, posting or downloading any information unrelated to their employment and, in particular, pornographic or other offensive material; and
- engaging in computer hacking and other related activities, or attempting to disable or compromise the security of information contained on the Employer's computers.

You are reminded that these activities may constitute a criminal offence.

Email

The use of the work email system (work email) is encouraged as its appropriate use facilitates efficiency. Used correctly, it is a facility that is of assistance to the Employer. However, inappropriate use causes a number of problems, including distractions, time wasting and legal claims. The policy sets out the Employer's position on the correct use of work email.

Unauthorised or inappropriate use of work email may result in disciplinary action up to and including summary dismissal.

Work email is available for communication and matters directly concerned with the legitimate business of the Employer. Employees using work email should:

- comply with Employer communication standards;
- only send emails to those to whom they are relevant;
- not use email as a substitute for face-to-face communication or telephone contact;
- not send inflammatory emails (i.e. emails that are abusive);
- be aware that hasty messages sent without proper consideration can cause upset, concern or misunderstanding;
- if the email is confidential, ensure that the necessary steps are taken to protect confidentiality;
- be aware that offers or contracts transmitted by email are as legally binding on the Employer as those sent on paper; and
- ensure that passwords are not sent across via email.

- The Employer will not tolerate the use of work email for unofficial or inappropriate purposes, including:
- any messages that could constitute bullying, harassment or other detriment;
- personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters);
- on-line gambling;
- accessing or transmitting pornography;
- social media;
- transmitting copyright information and/or any software available to the user;
- posting confidential information about other employees, the Employer or its customers or suppliers; or
- sending patients their medical results via email without the patient's written consent.

Monitoring

The Employer considers any and all data created, stored or transmitted upon the systems (the Systems) as work product and, as such, expressly reserves the right to monitor and review any data upon the Systems, including your usage and history, on an intermittent basis without notice.

In addition to this, the Employer has the right to protect its business interests and confidentiality. This includes the right to survey, audit and/or monitor its Systems, including but not limited to:

- monitoring sites users visit on the internet;
- monitoring time spent on the internet;
- reviewing material downloaded or uploaded; and
- reviewing emails sent and received.

Information reports will be available to the Employer which can subsequently be used for matters such as system performance and availability, capacity planning, cost redistribution and the identification of areas for personal development.

For the avoidance of doubt, we reserve the right to monitor all internet and email activity by you for the purposes of ensuring compliance with the Employer's policies and procedures and for ensuring compliance with the relevant regulatory requirements and you hereby consent to such monitoring. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

Social media

Whilst social media can be used to strengthen the Employer's brand and overall image of the business, work related issues or materials being placed on social media can adversely affect the Employer, a customer/client, colleague or others.

Social media is a mechanism for communication and sharing, rather than one specific program, activity or object. It is often a website or other electronic application that enable users to create and share content or to participate in social networking.

To protect the mutual interest of all involved, work related matters must not be placed on social media at any time either during or outside of working hours and this includes access via any mobile computer equipment, including mobile phone or other devices unless approved in advance. Work-related usually means that the Employer, its clients, suppliers, employees, contractors or any other associated parties can be identified and be in some way connected back to your relationship with the Employer.

All employees are prohibited from using social media (whether on the Employer's devices or their own personal device) during work time for personal reasons. You are not permitted to take photos on any client site.

Any breach of this policy will be considered serious and may result in disciplinary action.

MOBILE PHONES AND OTHER DEVICES

The Employer's mobile phones, laptops and other tablet devices are to be used for business purposes and incidental reasonable personal use.

Any unauthorised personal use may be repayable by you and may result in disciplinary action up to and including dismissal. The Employer reserves the right to deduct the appropriate sums from your salary in the event that repayments are not made.

Personal mobile phones, mp3 players and other personal devices should not be used during work time, other than in emergencies.

Surveillance

Surveillance may be conducted in the workplace. If you are a new employee the surveillance may already be in place and could start immediately on commencement of work.

Surveillance may be conducted using:

- internet usage recording devices, such as data capture, web browsing and email history captured on servers, and keystroke recognition
- any form of visual recording devices including all types of camera, such as CCTV cameras
- any form of audio recording devices and
- electronic recording devices in any part of the workplace.

The surveillance may be conducted at any time and any employee may be subject to surveillance. The surveillance may be continuous or intermittent at the Employer's discretion. The Employer may, at their discretion, disclose the surveillance records for any reason that is not barred by privacy legislation.

You may consult with the Employer regarding any concerns about the surveillance. All cameras are visible and recording devices (including cameras) will not be placed in bathrooms or change rooms.

The purpose of the surveillance is to ensure the safety and security of employees, visitors and property. The Employer reserves the right to review and use the CCTV in disciplinary proceedings.