Data Protection Policies

JLM Medical Services Ltd

# Contents

## Version History

| Version | Date | By | Notes |
|---|---|---|---|
| 1.0<br>1.1 | Fri 1 Jul 2022<br>Tue 14 Nov 2023 | Chris Thomas<br>Judith Mohring | Initial Version<br>Annual Review |

# 1 Scope & Objectives

These policies cover the JLM Medical Services ("JLM" or "The Company") business as a whole and primarily concerned with addressing the risks associated with people, processes, technology, and data. JLM is committed to maintaining and continually improving its protection of confidential information. These policies set out with the aim of achieving a safe, secure environment for data that is properly handled.

These policies apply to all data and information relating to the company business, as well as all hardware and software resources. Each JLM employee, subcontractor and associate is personally responsible for adhering to these policies. The Company may take disciplinary action against any person found to be in contravention.

Any suggestions, recommendations or feedback on these policies are welcome.

# 2 Key Responsibilities

- Dr Judith Mohring is the director and senior manager with overall responsibility for these policies.
- Kirsti O'Sullivan is the Administrator with day-to-day responsibility for implementing and ensuring compliance to these policies.
- ITF Tech Ltd is the IT partner used to facilitate operation and support of IT and related security.
- Run Robin Limited is the consulting partner used to assist with technical and process strategy

# 3 Policy Governance

## 3.1 Policy Review & Continual Improvement

In accordance with the Scope and Objectives of this policy, JLM commits to reviewing the company policies, Risk Mitigation Log and JLM Service Register at least annually. A Data Protection Diary will be kept for this purpose.

## 3.2 Data Protection Awareness

JLM commits to ensuring all new employees are made aware of the requirements of the Data Protection Policies, and that all employees are regularly updated on their awareness of them. This includes awareness of all obligations arising from regulatory bodies or legislation, such as the GDPR and Data Protection Act.

# 4 Privacy Policy

This policy refers to our commitment to treat information of employees, clients, associates, and other interested parties (collectively "you") with the utmost care and confidentiality.

## 4.1 Who We Are

JLM Medical Services ("We", "The Company") is registered in England, company number 09612209. Its principal place of business is Linear House, Peyton Place, London SE10 8RS and its registered address is 80 Ashton Road, Denton, Manchester, England, M34 3JF. The ICO Registration Number is ZA136707. The Company can be contacted regarding the privacy policy and data protection matters via the methods laid out in the Contact Us section.

## 4.2 Data Protection Officer

JLM does not require a Data Protection Officer as it is not a public body and does not carry out large-scale data processing.

## 4.3 The Data We Collect

We are committed to only collect and process the minimum personal data needed, and to ensure any processing of data is lawful, fair, and transparent.

We collect:

- email (and sometimes phone numbers) for those who attend webinars and workshops
- email and phone numbers for client contacts and contracts
- billing information

Should you wish to provide it, we may collect:

- your contact details, as provided in the 'contact us' form

## 4.4 Use Of Data

The Company will only use your data for the purposes necessary, where there is a legitimate interest or contracted services with you:

- To provide and maintain our services, and provide customer care and support
- To monitor the security of the website and address technical issues
- To identify you and your accounts and relationships with us
- To notify you, where requested, of service information

JLM will never use personally identifiable information provided to it in ways unrelated to those described above, unless you have provided consent for that purpose (e.g. contact details provided for sales or marketing purposes), which you have the right to withdraw at any time.

The company does not share any personal information with any third party, except:

- For the purposes of secure data storage (see 'Data Storage') or carrying out the contracted services
- Where it is necessary for carrying out regulatory or legal obligations (e.g. contract or employment), or for the legitimate interests of the company (e.g. debt recovery)

## 4.5 Data Storage

Your information is securely stored within the UK & EU by the Company's service providers. These third parties have limited access to personal data, only to perform these tasks on our behalf, and are obligated not to disclose or use it for any other purpose.

We retain all information while there is an ongoing relationship with you or your organisation and will review all data on termination of that relationship, deleting all data except that used to record a history of the relationship (e.g. Accounting data) or where obligated to comply with applicable laws.

## 4.6 Data Protection Rights

Under data protection law, you have rights including:

- **Your right of access** - You have the right to ask us for copies of your personal information.
- **Your right to rectification** - You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- **Your right to erasure** - You have the right to ask us to erase your personal information in certain circumstances.
- **Your right to restriction of processing** - You have the right to ask us to restrict the processing of your information in certain circumstances.
- **Your right to object to processing** - You have the right to object to the processing of your personal data in certain circumstances.
- **Your right to data portability** - You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you. You can correct factual errors in your information by sending us a request with credible evidence of error. To protect your privacy and security, we will take reasonable steps to verify your identity before granting access or making corrections. Please contact us at via the contact details if you wish to make a request.

If you are unsatisfied with our responses, you have the right to lodge a complaint with the Information Commissioner's Office at https://ico.org.uk

## 4.7 Children's Privacy

We do not knowingly collect personally identifiable information from anyone under the age of 18. If you are a parent or guardian and you are aware that your child has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we take steps to remove that information from our servers.

## 4.8 Links To Other Sites

Our website may contain links to other sites that are not operated by us. We have no control over those websites and cannot be responsible for the content or privacy for protection of those sites. We advise you to review the Privacy Policy of those websites, should you wish to follow the links.

## 4.9 Changes To This Privacy Policy

We may update our Privacy Policy from time to time and will notify you of any changes by posting the new Privacy Policy on our website. You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted.

## 4.10 Contact Us

For queries regarding this Privacy Policy, contact Dr Judith Mohring at judith@thenaturalpsychiatrist.com or JLM Medical Services Ltd, Linear House, Peyton Place London SE10 8RS

# 5 Data Storage & Processing Policy

Processing different types of information is key to the operation of the JLM business. This policy is aimed at ensuring data is handled appropriately, and that records are kept of what information the Company stores and processes.

## 5.1 Data Classification

To aid in identifying the appropriate handling for each type of data, a classification must be associated with each item of data. It is possible that an item encompasses more than one classification, at which point all applicable regulations and security must be considered.

The classifications are:

| | |
|---|---|
| **Personal** | Data that contains personal information of Employees or other identifiable persons (e.g. HR records, CVs, Client Lists) |
| **Proprietary** | Data that contains information that the company considers confidential and does not disclose externally, usually to prevent financial loss, give competitors an advantage, etc. (e.g. Accounting records, Internal Email) |
| **Client** | Data supplied or otherwise owned by clients, which the Company has been authorised to handle in the usual course of business (e.g. Company handbooks, Operational data) |
| **Unclassified / Public** | Data that is not restricted (e.g. Marketing materials, website) |

Data categorised as Personal must be handled in accordance with the regulations laid down in GDPR. Any suspected breaches of privacy regarding this data must be reported as soon as possible to the senior manager.

For Data categorised as Client, care must be taken to ensure the confidentiality of the data is maintained. Particularly, the data may be subject to a Non-Disclosure Agreement, or other contractual confidentiality requirements. From a GDPR perspective, JLM is the 'Processor' for this category of data - in all other cases, JLM is the 'Controller'.

Proprietary data should be handled securely and not disclosed to any third parties without prior consent from a senior manager.

## 5.2 Data Storage

JLM does not operate any servers or local data storage setups, other than personal computers. It does not operate any self-hosted systems or applications.

JLM uses secure third-party service providers to facilitate all data storage and hosting of applications that may contain or process data. Where third parties are storing data, their Privacy, Data and Security policies are inspected before use.

Anyone with access to data or emails must not forward the data outside of the company unless it is required to communicate legitimately with a third party for company business, or they have been

given permission from a senior manager.  For example, forwarding data or emails to personal accounts to facilitate working from off site is not permitted.

When storing general purpose data, such as in a file directory, the classification of data should be indicated to aid awareness of how it should be handled.

Removable storage, such as CDs or USB drives, are not permitted for use within JLM, except where needed by the IT Provider for technical support.

## 5.3 Registers Of Storage & Processing

A full catalogue of stored data, along with its classification, access and interested parties is maintained in the JLM Service Register.

# 6 Acceptable Use Policy

The purpose of this policy is to describe the acceptable use of JLM resources and information. This includes email, internet access, software, hardware, networks, office equipment and other tools used for carrying out JLM business.

It applies to all resources and all users of those resources, including Employees and third parties. Individuals are responsible for their own actions, and the use of JLM resources assumes and implies compliance with this policy.

JLM provides technology resources for the purpose of supporting the running of the business. These resources are set up according to the relevant security procedures, including Anti-Virus and other controls, and are optimised for the purposes of the business. Users given access to these resources must not interfere with or otherwise attempt to circumvent these protections.

Depending on the person's role, they may have access to passwords, access codes or physical security apparatus. Any such security code or device must only be used for the purpose for which it is intended, must not be shared or disclosed with anyone, and people in possession should maintain the integrity and confidentiality of these security devices. Should a password become exposed or device lost, the user must report this immediately to the senior manager in line with the Incident Management Handling Policy.

## 6.1 Personal Use

JLM allows the use of its resources by Employees for reasonable personal use. An exhaustive definition of reasonable use is beyond the scope of this policy, but includes that the activities:

- are not detrimental to the main purpose for which the facilities are provided
- do not interfere or compete with the company business
- are not commercial or profit-making
- are not abusive, offensive, or otherwise illegal
- are not at odds with any other company policy or regulatory restriction

Should there be any doubt about what constitutes reasonable use, consult a senior manager.

## 6.2 Receipt Of Inappropriate Or Offensive Content

Should an employee receive inappropriate or offensive content (e.g. via email or website) they should not communicate with the sender or source, not delete the data, and report the incident to a senior manager.

# 7 Security Policy

The security of information is very important to the Company, and our objective is to maintain its confidentiality, integrity and availability.

- Confidentiality means only authorised people can access the information, and unauthorised and external people cannot.
- Integrity means that information is accurate, complete, cannot be altered without correct processes applied, and is suitable for the purpose for which is used
- Availability means that authorised people have access to the data and resources when they need it

It is the policy of the Company to ensure that:

- All employees are aware that it is their responsibility to adhere to this policy
- All regulatory and legislative requirements are met
- All computer, data and information systems are protected against unauthorised or malicious access
- Breaches of the policy will be handled in accordance with Incident Handling policy

## 7.1 General Principles

A general set of principles applies across the Company with regards to default security:

- All access to computer equipment, software services or office space will be secured from unauthorised entry by passcodes or keycards
- Passwords, security devices, ID Keys and personal logins must not be shared, and must remain confidential to the user
- All screens, computer equipment, mobile devices and office spaces will be locked and/or secured while unattended
- Multi-factor authentication must be used where available
- All computer equipment will be securely set-up and decommissioned by the IT Partner
- The IT Partner will perform regular checks to ensure all computer equipment and services are operating normally and have the most regular updates
- The company, along with the IT partner will perform regular checks to ensure emergency/business continuity procedures are effective

## 7.2 Access Control

Further to the General Principles above, specific areas of the technology environment have further access controls.

The JLM policy towards access control works on the Principle Of Least Privilege. This means that people are only given as much access as they need to perform their duties (and no more), and thus minimising the risk of accidental or unauthorised access to secure resources.

As the company does not host any local data or servers, there is no remote access required.

### 7.2.1 Employee Onboarding

When employees join the company, they are subject to background checks appropriate to their position.

The Administrator follows the New Employee Procedure to methodically onboard the employee with the correct access, security setup and hardware. This procedure ensures consistent, reliable setup for each employee in line with the data policies.

The Administrator must keep a dated copy of the onboarding checklist (from the New & Leavers Employee Procedure) to certify and evidence that it has been completed.

### 7.2.2 Employee Leaving

When an employee leaves the company, the Administrator follows the Employee Leaving Procedure to methodically remove access and data associated with the employee and to retrieve hardware for decommissioning.

The Administrator must keep a dated copy of the leaving checklist (from the New & Leavers Employee Procedure) to certify and evidence that it has been completed.

### 7.2.3 Administration

The Administration is performed at two levels:

- Internal permissioning by the Administrator
- Security and hardware setup by the IT Partner

All access control is covered by the Administrator, plus any authorised deputies. The main data and email service is centrally controlled by the IT partner and logs relevant account activity in the central admin account.

The IT Partner uses Webroot management system to centrally control security and alerts against threats and other events.

## 7.3 Email

Email services are provided by Microsoft Office 365 / Google Workspace and protected by Advanced Email Threat Protection. Alerts and reports are immediately sent to the IT Provider where activated.

## 7.4 Network

As the company does not operate servers or offices, there are no applicable networks.

## 7.5 Anti-Virus & Encryption

As well as a secure setup, all hardware used within JLM must be fitted out with up-to-date anti-malware protection, as prescribed by the IT Partner.

## 7.6 Asset Management

The preferred computer systems for purchase are approved by the IT Partner. Exact specifications are beyond the scope of this policy (and in any case are likely to change over time and due to availability), but must include microphone, camera and speakers and be able to run the latest versions of Microsoft Windows, Office, and any other software used by the Company.

Decommissioning of IT hardware must be done under advice from the IT Partner, once collected by the Administrator.

All software must be authorised and correctly licenced for use within the company. Software licencing is managed by the Administrator, who keeps records to ensure compliance with this policy.

# 8 Clear Desk Policy

The Clear Desk Policy is aimed at reducing the amount of hardcopy records processed and thus reducing potential information risks.

When leaving their desk (such as, at the end of the day), employees are expected to ensure there are no classified documents on their desk and they are locked away in appropriate, secure cabinets or desks. This especially includes anything with Personal data on it, such as business cards.

Employees are expected to avoid printing documents if possible. Should they need to print documents, employees must retrieve the printouts from the printer as soon as possible.

All paper documents with Personal, Proprietary or Client data on them must be disposed of securely - for example by shredding or using a secure document disposal service.

# 9 Incident Handling

Any suspected breaches of the data policy - especially where GDPR or other regulation is concerned - should be reported immediately to the senior manager.

In the event of an incident leading to the loss or disclosure of personal data, the Company must promptly assess the risk and impact and, if appropriate, record an entry in the Risk Log and/or report to the Information Commissioner's Office within the mandated 72 hour window.

Failure to report suspected or actual breaches to the senior manager may result in disciplinary action being taken, and may also result in regulatory action being taken by the Information Commissioner's Office. A data privacy breach could result in potential fines to the company (20 million Euros or 4% of turnover), and cause serious reputational damage.

In the event of an incident leading to an issue with regulatory compliance, the senior manager must be notified.

Where an incident is caused by an employee behaviour, HR should be informed in case any disciplinary actions are required.