DATA PROTECTION POLICY PROCEDURE

PROVIDED BY:
MAT GROUP LTD.

DATA PROTECTION PPOLICY PROCEDURE

1. Introduction:

MAT Group Ltd. needs to gather and use certain information about individuals. These can include customers, trainees, Instructor(s), business contacts, employees and other people the organization 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. Personal Data is any information (including opinions and intentions) which relates to an identified or MAT Group's leadership is fully responsible for ensuring continued and effective implementation of this policy and expects all MAT Group Employees to share in this commitment.

2. Why This Policy Exists:

This data protection policy ensures MAT Group:

- 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

3. Scope:

This policy applies to all staff. MAT Group's staff must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to staff use of internet, email use and all existing information of clients in MAT Group Data systems. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Definitions:

Personal Data:

Personal Data means any information relating to an identified or identifiable individual (the "Data Subject").Personal Data includes all types of information that directly or indirectly may be linked to the Data Subject. Includes name, address, telephone number, and id number.

Sensitive Data:

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Data Controller:

Any person (or organization) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject:

Any living individual who is the subject of personal data held by an organization.

Processing:

Any operation related to organization, retrieval, disclosure and deletion of data and includes: Obtaining and recording data accessing, altering, and adding to, merging or deleting data.

Third Party:

Any individual/organization other than the data subject, the data controller (Training Company) or its agents.

Relevant Filing System:

Any paper filing system or other manual filing system, which is structured so that information about an individual is readily accessible.

It is to be note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

4. Data Protection Risks:

This policy helps to protect MAT Group 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.

5. Responsibilities

Everyone who works for or with MAT Group 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 board of directors is ultimately responsible for ensuring that MAT Group meets its legal obligations.
- The data protection officer Mr.Reza Nikdel 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 MAT Group Ltd. 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 IT manager, Mr.Reza Nikdel, 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.
- The marketing manager, Mr.Fareeman Golshan, is responsible for:
  - ✓ 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

6. 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. When access to confidential information is required, employees can request it from their line managers.
- MAT GROUP will provide training 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, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorized 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 their line manager or the data protection officer if they are unsure about any aspect of data protection.

7. 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 unauthorized 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 unauthorized people could see them, e.g. as on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

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

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (e.g. 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, away from general office space.
- 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 such as tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

8. Data Use:

Personal data is of no value to MAT Group 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, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorized external contacts.

- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

9. Data Accuracy:

The law requires MAT Group 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 MAT Group 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.
- MAT Group will make it easy for data subjects to update the information MAT Group holds about them. For instance, via the company website.
- 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.
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

10. Subject Access Requests:

All individuals who are the subject of personal data held by MAT Group 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.

If an individual contacts 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 controller at info@matgroup.org. The data controller can supply a standard request form, although individuals do not have to use this.

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

11. Disclosing Data for Other Reasons:

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

Under these circumstances, MAT Group will disclose the 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.

12. Providing Information:

MAT Group 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 (www.matgroup.org).

Policy Authorized By: **Date:** 10/02/2020

MAT Group Ltd.

Ali Amidi