Data Protection Policy

This document outlines the requirements for sourcing, storing and handling personal data in accordance with the General Data Protection Regulation (GDPR) 25th May 2018

The requirements set out in this document apply to persons and 3rd party entities who control or process data on behalf of Majestic Ventures LTD Ltd.

Important information:

Any contravention of this policy which constitutes a breach of the GDPR can incur significant penalties not only to Majestic Ventures LTD Limited but also to the individual who caused the data breach.

Violation of this policy is considered gross misconduct or at least gross negligence and is therefore grounds for dismissal or, in relation to 3rd parties, legal action.

Data Protection Policy

Context and overview Key details

Majestic Ventures LTD Ltd needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people 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 Majestic Ventures LTD Ltd:

- 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 General Data Protection Regulation (GDPR) describes how organisations — including Majestic Ventures LTD Ltd— 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 processed or disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. 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 Majestic Ventures LTD Ltd
- All branches of Majestic Ventures LTD Ltd

Data Protection Policy

- All staff and volunteers of Majestic Ventures LTD Ltd
- All contractors, suppliers and other people working on behalf of Majestic Ventures LTD Ltd

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 (GDPR). 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 Majestic Ventures LTD Ltd 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.
- **Financial penalty.** Organisations can be fined up to 4% of annual gross turnover or €20 million (whichever is greater)

Responsibilities

Everyone who works for or with Majestic Ventures LTD Ltd 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 Majestic Ventures LTD Ltd meets its legal obligations.

These roles and responsibilities for the primary data controllers and processors, however, it should be made clear that everyone within the company and those working on behalf of Majestic Ventures LTD Ltd have specific roles and responsibilities when it comes to processing data. The General Data Protection Regulation (GDPR) identifies certain roles and defines their responsibilities as: **Data controllers**

The natural person or legal entity that determines the purposes and means of the processing of personal data (e.g., when processing an employee's personal data, the employer is considered to be the controller). It is possible to have joint data controllers in certain circumstances. For example, when a company operates in multiple countries, but decisions on processing purposes are being made both by central and local entities, the scenario would qualify as a joint controller.

The key responsibility of a controller is to be accountable, i.e., to take actions in line with GDPR, and to be able to explain the compliance with GDPR to data subjects and the Supervisory Authority, as and when required.

Data Protection Policy

Data processor

The natural person or legal entity that processes personal data on behalf of the controller (e.g., a call centres acting on behalf of its client) is considered to be a processor. At times, a processor is also called a third party.

The key responsibility of the processor is to ensure that conditions specified in the Data Processing Agreement signed with the controller are always met, and that obligations stated in GDPR are complied with.

Assumed roles and responsibilities

When dealing with data on a daily basis individual will naturally assume one of the identified roles and therefore its responsibilities. In most cases members of staff will naturally assume the role of **data processor** in their day to day handling of customer data.

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.
- **Majestic Ventures LTD Ltd 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 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 their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data classification definitions

The following table provides a summary of the information classification levels that have been adopted by Majestic Ventures LTD Ltd and which underpin the principles of information security defined in the *Information Security Policy (Section 2.1)*. These classification levels explicitly incorporate the General Data Protection Regulation's (GDPR) definitions of Personal Data and Special Categories. **1. Confidential**

'Confidential' information has significant value for Majestic Ventures LTD Ltd, and unauthorised disclosure or dissemination could result in severe financial or reputational damage to Majestic Ventures LTD Ltd, including fines of up to 4% gross turnover (or €20 million – whichever is higher) from the Information Commissioner's Office, the revocation of rental or insurance contracts and the failure to win future business. Data defined by the GDPR as Special Categories of Personal Data falls into this category. Only those who explicitly need access must be granted it, and only to the least degree in order to do their work (the 'need to know' and 'least privilege' principles). When held

outside Majestic Ventures LTD Ltd, on mobile devices such as laptops, tablets or phones, or in transit, 'Confidential' information must be protected behind an explicit logon and by a suitable level (AES 256-bit) encryption at the device, drive or file level, or by other controls that provide equivalent protection.

2. Restricted

'Restricted' information is subject to controls on access, such as only allowing valid logons from a small group of staff. 'Restricted' information must be held in such a manner that prevents unauthorised access i.e. on a system that requires a valid and appropriate user to log in before access is granted. Information defined as Personal Data by the GDPR falls into this category. Disclosure or dissemination of this information is not intended, and may incur some negative publicity, but is unlikely to cause severe financial or reputational damage to Majestic Ventures LTD Ltd. Note that under the Data Protection Act large datasets (>1000 records) of 'Restricted' information may become classified as Confidential, thereby requiring a higher level of access control.

3. Internal Use

'Internal use' information can be disclosed or disseminated by its owner to appropriate members of Majestic Ventures LTD Ltd, partners and other individuals, as appropriate by information owners without any restrictions on content or time of publication.

4. Public

'Public' information can be disclosed or disseminated without any restrictions on content, audience or time of publication. Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the appropriate computer system.

Security Level	Definition	Examples	FOIA2000 Status*
1. Confidential	Normally accessible only to specified members of Majestic staff. Should be held in an encrypted state outside Majestic systems; may have encryption at rest requirements from providers.	GDPR-defined Special Categories of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record) including as used as part of rental or insurance agreements; driving license information; data used for card processing and payments; passwords; large aggregates of personally identifying data (>1000 records) including elements such as name, address, telephone number.	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.

2. Restricted	Normally accessible only to specified members of staff or authorised 3rd parties	GDPR-defined Personal Data (information that identifies living individuals including home / work address, age, telephone number, education, photographs); reserved management business; draft reports, papers and minutes; company asset information;	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
3. Internal Use	Normally accessible only to members of staff and authorised 3rd parties	Internal correspondence, company papers and minutes; vehicle and company asset information; information held under license;	Subject to scrutiny in relation to appropriate exemptions/ public interest and legal considerations
4. Public	Accessible to all members of the public	Annual accounts, minutes of statutory and other formal committees;	Freely available on the website or through Majestic publications
		information available on the KC website or through Majestic publications;	

Explicit data controllers and other rights of access to information

Majestic Ventures LTD Ltd recommends that branches, departments and authorised partners **explicitly designate data controllers and data processors**.

Other users may have rights of access to data according to the terms of engagement under which the data was gained or created.

Granularity of classification

The sets of information being classified should, in general, be large rather than small. Smaller units require more administrative effort, involve more decisions and add to complexity, thus decreasing the overall security.

Information Retention

There may be minimum or maximum timescales for which information must be kept. These may be mandated in a commercial or legal contract. Other forms of information retention may be covered by environmental or financial regulations.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can

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.

Data Protection Policy

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 or in a restricted locked room**.
- 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** 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.
- Data should not be stored on removable disks where possible, however, if data is **stored on removable media** (like a USB stick, 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 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 Majestic Ventures LTD Ltd 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 authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers or storage devices.** Always access and update the central copy of any data.

Data Protection Policy

Data accuracy

The law requires Majestic Ventures LTD Ltd 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 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 or copies of data.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- Majestic Ventures LTD Ltd will make it **easy for data subjects to update the information** Majestic Ventures LTD Ltd 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 available suppression lists** every six months.

Subject access requests

All individuals who are the subject of personal data held by Majestic Ventures LTD Ltd 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 protection officer at Reservations@majesticventure.com . The data controller can supply a standard request form, although individuals do not have to use this.

Individuals may be charged up to £10 per subject access request. The data controller will aim to provide the relevant data within 14 days or a maximum of 40 calendar days from receipt of the subject access request. There will be no charge to Majestic Ventures LTD Ltd employees for subject access requests.

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

Data Protection Policy

Disclosing data for other reasons

In certain circumstances, the General Data Protection Regulation (GDPR) allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Majestic Ventures LTD Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board of directors and from the company's legal advisers where necessary.

Providing information

Majestic Ventures LTD Ltd 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.