DATA PROTECTION POLICY

Castello Di Monte

Introduction

Castello Di Monte needs to gather and use certain information about individuals.
These can include clients /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 that Castello Di Monte:

- Complies with data protection law and follows good practice;
- Protects the rights of staff, customers / clients and partners;
- Is open about how it stores and processes individuals' data; and
- Protects itself from the risks of a data breach.

Data Protection Legislation

The Protection of Personal Information Act, 2013 describes how organisations, including Castello Di Monte, 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 disclosed unlawfully.

The Protection of Personal Information Act is underpinned by eight important conditions, and eight additional rights and obligations. These say that personal data must:

- Accountability;
- Processing limitation;
- Purpose specification;
- Further processing limitation;
- Information quality;
- Openness;

- Security safeguards;
- Data subject participation;
- Processing of special personal information;
- Processing of personal information of children;
- Direct marketing by means of unsolicited electronic communications;
- Automated personal information processing;
- Trans-border information flows;
- Outsourcing personal information processing;
- Appoint and duties of the information officer; and
- Prior authorisation;

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of Castello Di Monte;
- All staff and volunteers of Castello Di Monte; and
- All contractors, suppliers and other people working on behalf of Castello Di Monte.

It applies to all data that Castello Di Monte holds relating to identifiable individuals, even if that information technically falls outside of the Protection of Personal Information Act, 2013. 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 Castello Di Monte 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 Castello Di Monte uses data relating to them; and
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Castello Di Monte has some responsibility for ensuring data is collected. Stored and handled appropriately.

Each person / 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 directors / executive management is ultimately responsible for ensuring that Castello Di Monte meets its legal obligations
- The Information Officer / Data Protection Officer, is responsible for:
    - Keeping the board / executive management 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 everyone else covered by this policy;
    - Dealing with requests from individuals to see the data Castello Di Monte holds about you; and
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The IT Manager and IT Service Provider, are 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, 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; and
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

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 if from their managers;
- Castello Di Monte **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, whether 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; and

- Employees **should request help** from their managers or the data protection officer 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 IT Provider /IT Manager / Deputy Information Officer.

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**;

- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer, fax machine, scanner or your desk;

- **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 employees;

- If data is **stored on removable media** (like a CD, DVD flash drive or removable hard drive), 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 service**;

- 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; and

- All servers and computers containing data should be protected by **approved security software and a firewall or two.**

Data Use

Personal data is of no value to Castello Di Monte 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 South Africa**; and

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

Data accuracy

The law requires Castello Di Monte to take reasonable steps to ensure data is kept accurate and up-to-date.
The more important it is that the personnel data is accurate, the greater the effort Castello Di Monte 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, be confirming a customer's / client's details when they call;

- Castello Di Monte will make it **easy for data subjects to update the information** Castello Di Monte holds about them.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer / client can no longer be reached on their stored telephone number, it should be removed from the database; and

- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject access requests

All individuals who are the subject of personal data held by Castello Di Monte 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**; and

- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts Castello Di Monte, requesting this information, this is called a data subject access request.
Data subject access requests from individuals should be made by email, addressed to the information officer / deputy information officer at Privacy@Bluediamond.co.za.The information officer / deputy information officer can supply a standard request form.
The information officer / deputy protection officer will aim to provide the relevant data within 14 days.
The information officer / deputy protection officer will always verify the identity of anyone making a data subject access request before handling overt any information.

Disclosing data for other reasons

In certain circumstances, the Protection of Personal Information Act, allows personnel data to be disclosed to law enforcement agencies without the consent of the data subject.
Under these circumstances, Castello Di Monte, will disclose requested data. However, the information officer / deputy information officer, will ensure the request is legitimate, seeking assistance from the board / executive and from the company's legal advisers where necessary.

Providing information

Castello Di Monte aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used; and

- How to exercise their rights.

To these ends, Castello Di Monte has a privacy statement, setting out how data relating to individuals is used by Castello Di Monte.